ITSD Technical Architecture

Ernest Orlando Lawrence Berkeley National Laboratory
Berkeley, California

October 25, 2002

This work was prepared for the U.S. Department of Energy under Contract No. DE-AC03-76SF00098.

TABLE OF CONTENTS

1. Introduction

The purpose of this document is to provide guidelines for the development of Ernest Orlando Lawrence Berkeley National Laboratory's information technology (IT) architecture based on the Laboratory's IT requirements, technology trends, and cost-effectiveness. This Technical Architecture has three primary goals:

- To define an IT infrastructure that efficiently and effectively supports the Laboratory's scientific mission.
- To establish expectations for customers, technical staff, and management by creating a framework for the identification and prioritization of needed technology initiatives for a five-year time horizon.
- To help establish IT priorities and focus limited resources for both ongoing services and R&D projects.

The Architecture will be updated quarterly to keep pace with changing technologies and Laboratory needs.

This document takes into account user needs and requirements and provides guidelines and a decision-making resource for three groups: ITSD staff, the Operations Directorate, and IT customers throughout the Laboratory.

1. ITSD staff will use the Technical Architecture as a reference and guide when making decisions to acquire or adopt a technology. Technologies that do not fit within the current Architecture should be presented to the Technical Architecture Working Group to evaluate their appropriateness and suitability.
2. For the Operations Directorate, the Technical Architecture establishes the IT infrastructure that supports operational goals, optimizing the business benefit while controlling technology costs. Since available financial resources set limits on technology and service decisions, the Architecture provides a basis for prioritizing technology investments.
3. For customers of the IT infrastructure and services throughout the Laboratory, the Architecture serves as a guide for technology planning and decision-making, reflecting user needs and requirements. Use of recommended technologies and data formats will result in cost-effective and secure technology service delivery and support.

2. Current Situation

BACKGROUND

ITSD's infrastructure mission is to provide Berkeley Lab with efficient, effective, and innovative information technologies and services to enable world-class science. This document is the first version of an architecture for the Laboratory's technology infrastructure. It defines an integrated approach across all areas of Berkeley Lab's IT infrastructure. This plan builds upon the substantial technology benefits that the Laboratory has realized during the past decade and incorporates the modern technologies we need to remain at the forefront of scientific research. In addition, this plan incorporates a range of services that encompasses virtually all areas of modern computing and communications technology (with the exception of large-scale scientific computing and programmatic efforts, i.e., ESnet and CEDR).

The largest strategic challenge facing ITSD is sustaining the effectiveness and dealing with the growth of these services in the face of rapid technology advancements and obsolescence that characterize IT functions. New and sometimes conflicting technology standards compound the decision-making challenge. The stability of the computing environment must be balanced with ever-increasing changes to the technologies currently on the market with "even better" emerging technologies and standards. Funding and budget limitations will be a constant factor in the planning process. These conditions create extreme challenges for ITSD in delivering timely and cost-effective information and technology services.

MODERNIZATION OF SYSTEMS

Beginning in 1995, a plan was undertaken to modernize all of the Laboratory's business systems. A large number of systems that contributed to high operating costs were in use. They used various methods for storing data. Most were designed and developed by contract and career staff. The 1995 plan proposed to replace and consolidate these many systems with third-party commercial application systems. These new third-party systems would store their data on Oracle databases. Expensive IBM mainframe software would be replaced with cost-effective UNIX servers. Huge numbers of expensive paper reports would be eliminated.

In 1997, reliance on workgroup software for electronic mail (e-mail) and meeting calendar management was increasing. The software, however, was not designed for or capable of handling the increasing volumes. Therefore, the Laboratory evaluated and acquired standards-based e-mail and meeting calendar software from Netscape Corporation. Netscape was the leading provider at that time. A major effort resulted in the majority of Berkeley Lab users converting to these Netscape products.

Progressing into the late 1990s, most users found that the new modern business systems and an increasing availability of information over the Internet improved their effectiveness. The Web browser became an increasingly important tool. The ubiquitous use of Web browsers for information access requires robust tools for authoring, management, and retrieval of this information. In 2002, the Technical and Electronic Information Department (TEID) acquired Virage, an online presentation technology that combines high-quality video streaming with other online media, which allows content owners to efficiently and rapidly digitize, manage, search, retrieve, and distribute video and other rich media assets. Web authoring also requires publication tools that can cross a diverse array of platforms. OpenType is a new cross-platform font file format developed jointly by Adobe and Microsoft that can support widely expanded character sets and layout features. Adobe Portable Document Format (PDF) is an open document format capable of electronic document distribution worldwide. It preserves the fonts, formatting, graphics, and color of any source document, regardless of the application and platform used to create it.

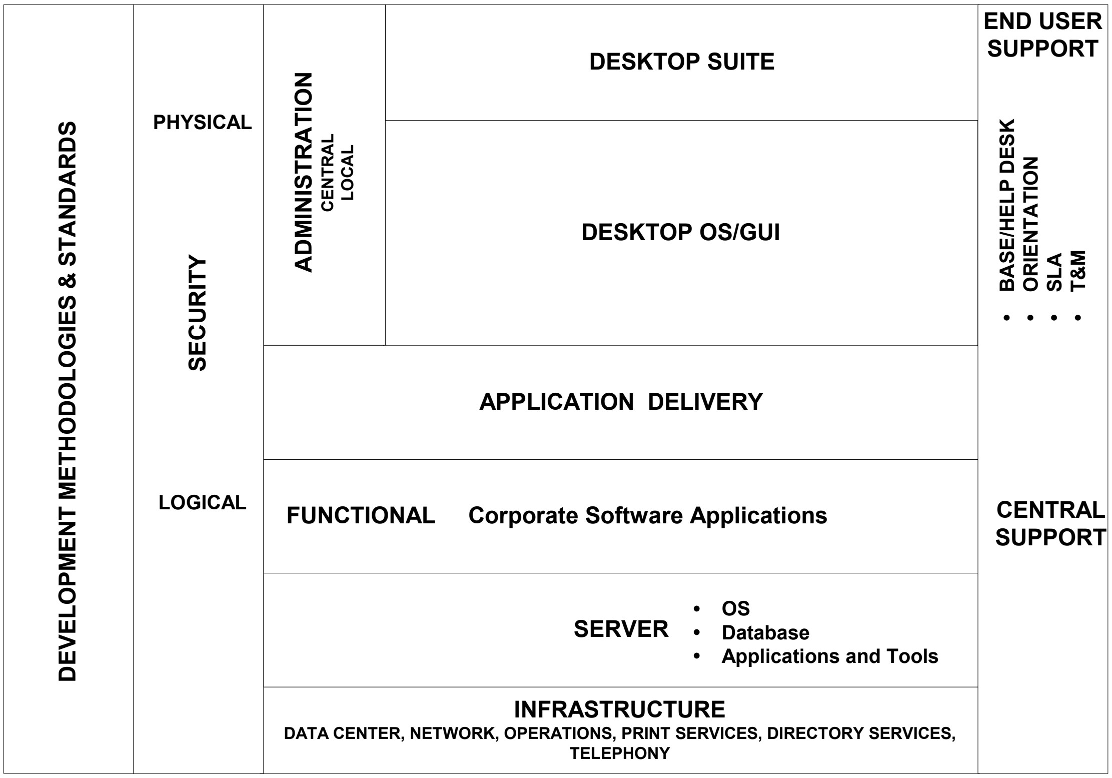
Prior to 1990, automation within the library consisted of DOS-based, networked PCs and mainframe applications. These homegrown programs automated parts of library functions. In the 1989–1990 timeframe, a Laboratory-wide committee evaluated and selected a general purpose, text-centered database management system with a library automation package built on top of the DBMS. The library DBMS and associated library automation package started out running on a VAX under VMS and were migrated to a Sun Solaris machine. The old Sun Solaris machine is soon to be replaced by a new server. The DBMS and library automation package are being upgraded to the latest versions. Most library services are now delivered to the user's desktop. The user still needs to visit the library for items that are not available electronically.

As the Laboratory enters the twenty-first century, the rapidly changing technology world poses significant opportunities and challenges. The Technical Architecture will help position ITSD and Berkeley Lab to capitalize on the opportunities technology offers.

3. Context Guide to the Technical Architecture

The following diagram provides a contextual view of the Technical Architecture. It consists of "layers" and "pillars." It is intended to show the relationship among the various components of the Technical Architecture. Starting with the bottom layer, the Infrastructure layer is the foundation. Each successive layer builds upon all lower layers. The Server layer depends and builds on the Infrastructure layer, and so on. Meanwhile, the pillars represent functions that apply to all the layers they span. For example, both Security and Support (including the Help Desk) impact all components of the Technical Architecture.

LOGICAL VIEW OF THE TECHNICAL ARCHITECTURE COMPONENTS



DEVELOPMENT METHODOLOGIES & STANDARDS

PHYSICAL

SECURITY

LOGICAL

ADMINISTRATION
CENTRAL
LOCAL

DESKTOP SUITE

DESKTOP OS/GUI

APPLICATION DELIVERY

FUNCTIONAL Corporate Software Applications

SERVER
- OS
- Database
- Applications and Tools

INFRASTRUCTURE
DATA CENTER, NETWORK, OPERATIONS, PRINT SERVICES, DIRECTORY SERVICES, TELEPHONY

END USER SUPPORT
- BASE/HELP DESK
- ORIENTATION
- SLA
- T&M

CENTRAL SUPPORT

The following sections of this document present:

- Summaries of key technology trends,
- A timeline for proposed initiatives, and
- Detailed descriptions of the Technical Architecture components.

4. Summaries of Key Technologies

INFRASTRUCTURE SERVICES AND APPLICATIONS

The Laboratory will continue to evaluate e-mail server and calendar products and reduce the number of required accounts/passwords by reducing the number of authentication sources, or by developing the ability to synchronize the ones that must remain. Internet Explorer will be supported as the default browser for corporate business systems. Methods will be developed to automate the distribution of security patches to desktop clients.

TELECOMMUNICATIONS AND VIDEOCONFERENCING

The Network and Telecommunications Department (NTD) is staying current with telephony technology trends. Voiceover IP (VoIP) is being continually evaluated to determine its viability within Berkeley Lab. A project is in the planning stages to upgrade the building wiring infrastructure to current standards. The telemanagement system is being replaced with a standards-based Oracle database. The Private Branch Exchange (PBX) upgrade will be completed mid-October 2002. NTD is negotiating with cellular service providers to develop an in-building wireless voice communications solution for Berkeley Lab.

FILE AND PRINTING SERVICES

ITSD has a limited role in Windows NT support for the Laboratory, but a significant investment in Novell file and print services. It is not clear what the future of Novell will be in this market. We are preparing for a change in direction by supporting our scientific users with a conversion of the NT4 domain environment to Windows 2000/Active Directory (AD) and building the expertise required if a change from Novell is warranted in the future. We are also modernizing support for UNIX Distributed printing with the deployment of the new Common UNIX Printing System (CUPS) technology.

ENTERPRISE NETWORKING

Berkeley Lab’s enterprise networking infrastructure is a critical resource for its operation and research activities. Its growth is inevitable due to the ever-increasing demands of its clients, and as such, congestion and outages become increasingly costly. Thus, operational reliability is critical to minimize costs to the Laboratory. In addition, new services (e.g., wireless networks, IPv6) must be considered for researchers with modern research facilities. The effort and materials required to support and grow LBLnet are ongoing, with engineering research an important part of this effort.

DATABASE SOFTWARE

All administrative systems are currently using Oracle databases. We foresee no changes in this area for the next three years.

OPERATING SYSTEMS

Windows XP Professional is the current desktop standard for administrative/business customers. For the next few years, older legacy Microsoft (Windows 98 and above) and Apple (Mac Version 9) operating systems will be supported. Mac OS X (based on the Berkeley Software Distribution — BSD), the Red Hat distribution of Linux, and SUN Solaris will become the only supported UNIX operating systems.

DESKTOP SOFTWARE

Microsoft Office is the standard Office Productivity Suite for PC users of the Windows operating system. The StarOffice product (based on the Open Office code base) will become the standard for UNIX/Linux users. Interoperability between Microsoft Office and StarOffice will be determined over the next year. Norton AntiVirus will continue to be the primary defense against virus attacks and will be provided via a site license. Static content for Web sites will standardize around Dreamweaver. Desktop firewalls for the Windows environment will be investigated in the future and compared to the capabilities built into Windows XP (Internet Connection Firewall — ICF).

WORKGROUP COLLABORATION

We will evaluate the potential benefit of workgroup collaboration software by investing in commercial Web-based software, developing several pilot projects, and identifying the cost/ benefit for internal as well as external use.

SECURITY

Trends in security technology include increased use of staging servers, increased use of third-party authentication methods, much-improved intrusion detection technology, and the emergence of methods that secure wireless networking. Staging servers are used, and will be used increasingly, to push software and security updates to remote systems, whereas third-party authentication, using additional authentication methods (e.g., smart card–based authentication) that are not provided by operating systems, will be tested for possible use at Berkeley Lab. Intrusion detection technology has grown considerably in sophistication; Berkeley Lab will examine alternatives to its homegrown Bro intrusion detection system, and will also continue to improve Bro capabilities. New authentication and encryption methods designed for wireless technology have the potential to considerably reduce the risk of using wireless networks.

BUSINESS SOFTWARE DEVELOPMENT AND DEPLOYMENT

The Laboratory will continue with its strategy to acquire business applications from commercial vendors and reengineer its business processes to adopt and utilize the “best industry practices” designs of the software. When our business processes are far removed from industry, we will develop applications using JSP and Java. All applications, acquired or developed, must be thin-client and Web-deployed.

SUPPORT SERVICES

We will continue to support and improve the central backup service for Berkeley Lab customers. In addition, we will develop a more integrated approach to customer service by synchronizing the computer training we offer with the standards we support and the services we offer through our Help Desk and support groups. We will also evaluate potential improvements to services we provide to off-site users (on travel or at home).

MULTIMEDIA, PUBLISHING, AND ARCHIVING SERVICES

Information is no longer just text, or text with static images. Information now comes in all forms and combinations — sound, video, virtual reality, etc. We need the ability to create, store, archive, retrieve, and deliver on demand this new type of information.

Parts of this effort entail the continued use of Virage for digitizing, managing, retrieving, and distributing video and other rich media assets; establishing a QuickTime server; negotiating volume or site licensing for Adobe Acrobat as well as providing training for it; adopting OpenType fonts when appropriate; acquiring a standards-compliant server if possible; and migrating the archives-and-records-management database to a DOE-compliant product or to Oracle.

5. Proposed Initiatives

Funding Classes:
Class A: Less than $50k
Class B: Between $50k and $100k
Class C: Between $100k and $250k
Class D: Greater than $250k
Blank: Included in the base

Initiatives	Timeframe For Completion (End Of Fiscal Year)					Funding Class
	02	03	04	05	06	
Infrastructure Services and Applications						
Recommend replacement alternatives for iPlanet e-mail server.		x				A
Support a single sign-on capability for Web-deployed corporate systems.		x				B
Implement a workable LDAP failover capability.			x			A
Telecommunications and Videoconferencing						
Evaluate voice recognition/authentication.		x				
In-building wiring upgrade.				x		
Evaluate a wireless-office voice application.			x			
File and Print Services						
Replace current NT4 Domains with Windows 2000 Active Directory.			x			C
Implement browser-based access to Novell file systems.		x				
Convert all printing systems to IP (including UNIX DP).		x				A
Eliminate the Novell NDS structure and fold into Windows 2000/Active Directory (AD).					x	C
Hardware						
Review future of PDA devices at the Lab.	x					
Recommend and support a Linux cluster platform for workgroup and departmental computing needs.		x				B
Publish a list of recommended printers.		x				
Enterprise Networking						
Upgrade network access in institutional common areas.		x				C
Upgrade building network feeds.			x			D
Install an IPv6 test bed.			x			B
Operating Systems						
Continue to evaluate issues related to Mac OS X.		x				
Discontinue support for IRIX and Tru64.			x			
Desktop Software						
Evaluate alternatives for the Microsoft Office desktop suite.		x				A

Workgroup Collaboration						
Evaluate workgroup collaboration software (e.g., eRoom)		x				A
Security						
Evaluate and recommend personal desktop firewall software for Wintel machines.		x				
Test methods for securing access to business sensitive data (e.g., smart cards).			x			C
Review alternatives/additions to Bro for intrusion detection.		x				B
Expand security requirements beyond UNIX by including Windows OS in the Regulations and Procedures Manual (RPM).		x				
Evaluate strong authentication alternatives.			x			A
Evaluate wireless Ethernet perimeter protection.		x				B
Business Software Development and Deployment						
Upgrade all vendor-supplied software to Web-deployed, thin client.			x			D
Convert in-house developed client/server applications to Web thin client technology.					x	D
Evaluate JSP, Java, and relevant development environments (JBuilder, WebSphere Studio, JRun Studio) for enterprise systems.		x				A
Define and publish a software design and development guideline.		x				
Support Services						
Support development of a new employee training program for computing services.		x				
Re-evaluate the use of centralized support for UNIX and enterprise file and print services within ITSD.		x				
Complete implementation of central backup service.		x				B
Multimedia, Publishing, and Archiving Services						
Upgrade the multimedia service.			x			A
Upgrade the Basis Library server and license.			x			B

6. Technical Architecture Components

Infrastructure Services and Applications

DESIRED STATE

- A synchronized directory service that supports a single sign-on
- A reliable, scalable, functional, and operable mail server and calendaring system that can be integrated with other corporate applications
- Minimal number of directory services

CURRENT STATE

Electronic Mail, Calendaring, and Directory Services

Berkeley Lab has used the same electronic mail, calendaring, and directory services software for the past four years.

A significant amount of standardization has been achieved in the electronic mail area, as over 85% of Berkeley Lab customers have converted to the use of Netscape. During the past year, the electronic mail component of Lotus Domino (Notes) was evaluated; however, it was not considered to be a viable contender for potential replacement of the Netscape product.

A move to Steltor, the original provider of the Netscape (iPlanet) calendar product, has been made. The company recently merged with Oracle Corporation. A good Web interface and a new client are now both available.

At least six primary directory services exist: Microsoft's Active Directory, Lightweight Directory Access Protocol (LDAP), Netware Directory Services (NDS), PeopleSoft, the NT master domain, and UNIX Network Information Services (NIS). All, with the exception of Active Directory, are used at the Laboratory.

Considerations

- NDS has a more complete directory capability than Active Directory. While Novell, the NDS vendor, has a questionable future, the next two years appear to favor NDS.
- Microsoft's Active Directory does not yet deliver the functionality available from NDS.
- Netscape's LDAP services are used by corporate applications like mail, calendar, and IRIS for user authentication.

The issue facing the Laboratory is whether to standardize on a single directory service implementation or plan for some kind of synchronization of the directory services that we intend to support. In addition, continued use of the current Netscape LDAP solution for user authentication of ISS corporate applications has already begun.

At this point, no investigative work has been done to look into UNIX use of LDAP for authentication.

Browsers

- Netscape
  - Current Netscape in use (version 4.75) is no longer supported
  - Has centralized management capabilities
  - Certificates (security) are easier to deploy
  - Is supported on many different platforms (Windows, Macintosh, flavors of UNIX)
  - Is losing market share
- Microsoft Internet Explorer
  - Does not support Linux OS
  - Does support Solaris
  - Is possibly more stable than Netscape
  - Is gaining market share (almost 80% at the present time)
- Gecko
  - Is the new open source version of Netscape
- Opera
  - Has a very small market

Considerations

The requirements for a desktop browser include:

- Support Web-enabled thin client applications
- Support HTTP/HTML/XML
- Support Java Virtual Machines (JVM)
- Support corporate applications
- Support E-commerce
- Support industry standard e-mail
- Be compatible with commercial third party application software

Web Server Software Platforms

The following Web server software platforms are currently in use at the Laboratory:

- Netscape
- Apache
- Microsoft Internet Information Services (IIS)
- Oracle Web Server

Netscape is used for the Laboratory Web server. Apache is used to support the IRISv2 application. IIS is used for some of the internal Web applications developed by ISS and by many individuals at the Laboratory. In the future, Oracle Web servers will be discontinued when the Sunflower (AMS property management) system reports can be removed from them.

TECHNOLOGY TRENDS

Browser Use

By browser (total sessions: 167,064). Data garnered from a large California Banking Institution (as of January 22, 2001):

- Microsoft Internet Explorer use: 135,238 sessions (80.94%)
- Netscape use: 31,783 session (19.02%)
- Other browser use (e.g., Opera): 43 sessions

In a similar review conducted in the spring of 2002, the percentage of Netscape users had dropped to 10%.

Cross-platform issues will involve not only the Mac, but also all the UNIX variants. Even if we develop to the thin client model with a specific browser, we might still need to delay a rollout if the latest version of the browser is not implemented on all the supported platforms.

Some software, like the current electronic mail and calendar products, may continue to have both local client and Web access. To the extent that client software is developed, the Laboratory may be limited in the number of Desktop Operating Systems that can be utilized.

Multiple OS support can cause delayed rollout until implementations for all are done (particularly if interoperability between different versions is an issue, like it was for Office 95–97).

Although these trends are for users external to Berkeley Lab, they are important for two reasons:

- They dictate what commercial vendors will support; and
- Some users of Laboratory resources are external to the Laboratory, using browsers that they might have at work or home (for example, users of the Laboratory's Job Opportunities listings).

AV Support

A RealAudio Server maintained by NTD supports the distribution of presentations captured by software such as the TEID Virage system. There have been some technical difficulties using Real with Internet Explorer. Similarly, Windows media player works on Windows systems, but not on other platforms. QuickTime may be the only true cross-platform software in this area.

RECOMMENDATIONS

The technology that supports infrastructure services is dynamic. The Laboratory should evaluate this technology to ensure that we are providing cost-effective, state-of-the-art services.

- Evaluate alternatives to Steltor (Oracle) calendaring at the same time the mail product is reviewed.
- Evaluate the possibility of consolidating and/or synchronizing the number of directory services.

- Support Internet Explorer as the default browser for the future development of corporate applications. Evaluate potential alternatives for the iPlanet e-mail server.
- Continue support for Netscape and Apache Web services for future corporate application development.
- Upgrade Netscape to the latest version.
- Phase out the use of the Oracle Web Server after the legacy applications that it supports no longer need it.
- Minimize the use of IIS.
- Review the use of QuickTime to support Laboratory-wide distribution of AV files.
- Use an automated mechanism to deploy operating-system service packs and patches to Windows desktops.

Telecommunications and Videoconferencing

DESIRED STATE

Voice Communications Switch

A voice recognition/authentication application that replaces the need for Help Desk staff to handle calls that can be resolved via automation. This offers 24/7 availability for a portion of the services offered by ITSD. For example, passwords can be reset remotely any time of the day or night.

Voiceover IP (VoIP)

VoIP can provide the same system reliability as a circuit-switch PBX, and can make telecommuting seamless. Offsite locations and telecommuters can be connected via the network. Telecommuters can plug in their telephone anywhere on the network, and have their Laboratory extension and features with them.

Infrastructure

Telco closets that have proper space and environmental systems necessary to provide redundant, uninterruptible service. Internal wiring that is category 5E or better to accommodate today's higher network bandwidth requirements.

Telemanagement System

A telemanagement system that allows telephone coordinators direct access to the database to request service, eliminating the need for the request to be retyped by Telephone Services staff. The system should be capable of sending automatic e-mail notification, providing the requester with a service order number and a due date. There should be a robust Web interface for telephone recharge information, allowing ad hoc queries and report generation.

Wireless Communications

Wireless communications that offer employees the option of carrying one device for all their communication needs. By having only one device, employees could take their Laboratory extension with them anywhere on site, increasing productivity and accessibility. This would require a fully integrated Cellular-PBX integration, and increased wireless data speeds.

Videoconferencing

Videoconferencing and videostreaming that are available on the desktop through a standard product. This would provide the ability to offer desktop training for the Environment, Health & Safety (EH&S) Division and others. In addition, all employees would be able to view Dr. Shank's addresses.

Small, portable videoconferencing equipment that is available for use in any conference room, allowing greater flexibility in scheduling.

CURRENT STATE

Voice Communications Switch

The Networking and Telecommunications Department (NTD) is currently in the process of upgrading the Laboratory's existing PBX, an Intecom S/80, to an Intecom Millennium E Switch. The Intecom S/80 utilizes a proprietary operating system and has limited Computer Telephony Integration (CTI) capabilities. The S/80 has been discontinued, and its service support will be discontinued in December 2002.

Voiceover IP (VoIP)

VoIP does not have a Quality of Service (QOS) that is satisfactory for full-scale deployment of large enterprise systems such as the Laboratory's. Although it is commonly installed for smaller systems, or for connecting a remote location that did not already have a telephone infrastructure in place to a large PBX, VoIP does not offer comparable reliability to a Telephone PBX, which has a QOS rating of "five 9s," meaning that it is 99.999% reliable. VoIP networks are only 99.9% reliable. This reliability translates to 5.25 minutes, or 525.6 minutes (8.76 hours) of downtime per year. The higher reliability of a PBX is the result of full redundancy of all critical components, the fact that all critical components are centrally located, and a continuous source of power (UPS and generator). Data networks, including LBLnet, are scattered throughout the buildings they support without redundancy and uninterruptible power sources.

Infrastructure

The current wiring infrastructure supporting both voice and data is comprised of primarily category-3 wire supporting 10 Mbs, and category-5E wire in a few locations supporting 1 Gbs. In addition, the telco closets housing the wiring infrastructure do not meet industry standards. In some cases, the current telco closets share space with the custodians' closets. This has presented some service issues, as part of the network has been accidentally disabled.

Telemanagement System

NTD's telemanagement system, a database utilized for billing, work order, infrastructure, and repair tracking/processing, is a proprietary database operating in a host/server environment. It is unable to accommodate Berkeley Lab's parent-child project ID relationship, as it treats all projects as a parent. The database is not Web-enabled, so there is limited access by data to customized Web applications outside the database.

Wireless Voice

Currently, there is not a suitable wireless voice application available on the market. This application would allow Laboratory staff to utilize one device for both cellular coverage and Laboratory telephones. Although NTD has tested a couple of systems manufactured by Nortel and Hughes, both manufacturers have discontinued their product, and NTD has removed the hardware supporting the application.

The availability of wireless voice at Berkeley Lab is further complicated by the lack of cellular coverage on our site. NTD is working with the major cellular providers to address the coverage issue. However, the process remains in the design stage, and the final frequency technology has not been identified, nor has funding been finalized.

Videoconferencing

Berkeley Lab currently supports three public videoconference rooms and one roll-around unit, which is used for large institutional rooms. All of the Laboratory's videoconference equipment supports both H320 ISDN and H323 IP-based connections. Currently, the majority of conferences are held using the H320 ISDN dial connections. Minimal desktop videoconferencing exists at the Laboratory as older videoconference systems had poor audio and video plug-ins for the desktop.

Primary users have been personnel from the Physics and Environmental Energy Technologies Divisions.

TECHNOLOGY TRENDS

Voice Communication Switches

The market is showing sustained growth in the large PBX arena. Manufacturers are starting to utilize standards-based servers to support the operations system. However, the actual programming that provides communication services is still proprietary. Major players in the large-system (above 3,000 lines) market continue to be Nortel, Avaya, Intecom, and Siemens.

Voiceover IP (VoIP)

VoIP is making some headway in the small-system (500-line and under) market. However, the large-system market has yet to welcome VoIP as a reliable option to the PBX. VoIP is attempting to deal with the reliability issue with some success in the hardware. Unfortunately, the hardware is dependent on the infrastructure to deliver the service. In most cases, the infrastructure for networks was not designed to reliably handle voice traffic as consistently as it handles PBX.

Infrastructure

A majority of corporations, universities, government agencies, etc., are attempting to upgrade their wiring infrastructure to support today's higher-speed networks. These organizations are installing category-5 enhanced wire for both networks and telecommunications to allow for greater flexibility in planning. Category-5E wire can accommodate network speeds of 1 gigabit per second. Telco closets are being redesigned with proper environmental systems to support network quality of service demanded by VoIP. This includes Heating, Ventilation and Air Conditioning (HVAC), UPS, and redundant hardware.

Telemanagement System

Most telemanagement developers have moved away from the host/server and client/server applications, and are migrating to a Web-enabled product. The goal is to allow easier retrieval of stored data as well as to offset the inputting of requests to the requester by providing online access to applications. In addition, the database structure for some of the major players is no longer proprietary. For example, Pinnacle, one of the largest developers, uses an Oracle database for its applications.

Wireless Voice

The wireless-office-application market is stagnant; its carriers are currently not willing to take the financial risk to build the infrastructure to support the service. Until a hardware manufacturer develops a product for customers' customized applications, they are not jumping at the bit to fund the installation. Manufacturers want to develop an out-of-the- box application.

Videoconferencing

Many locations, both government and private, are moving towards H320 IP-based videoconferencing. Some desktop videoconferencing is beginning to emerge at the Laboratory and elsewhere, as a few of the primary videoconference equipment manufacturers now sell standards-based H323 systems with high-quality audio. Laboratory division executive staff members are beginning to use videoconferencing for Directorate and division review meetings.

RECOMMENDATIONS

Voice Communications Switch

Continue with upgrade of the Laboratory's existing PBX. When the upgrade is complete, the PBX will be capable of supporting current telephony standards, including VoIP. The Laboratory realizes substantial cost avoidance, and there is little user disruption. The useful life cycle of the PBX is 7–10 years.

Integrate a voice recognition/authentication application to improve delivery of routine services such as password resets

Voiceover IP (VoIP)

Continue to test new applications as they are released. Budgetary dollars will be earmarked within Telephone Services to stay current with the technology, and to fund the testing of new hardware and software applications. Currently, VoIP should not be considered a viable alternative to replace the infrastructure and PBX in place today. It is not capable of supporting the quality of service demanded of voice communications.

Infrastructure

Replace the aging category-3 wiring infrastructure with category-5E or the current standard at time of installation. Upgrade the telco closets to the standards required to support category-5E wiring and VoIP network requirements. This will require enlarging some of the existing closets, constructing new closets, and no longer sharing closet space with Custodial Services. Proper cooling and uninterruptible power will be required in all closets if VoIP is ever to be considered an option.

Telemanagement System

Replace the existing host/server proprietary database with an application that is Web-enabled utilizing an off-the-shelf database. Provide customers direct access to specific fields to eliminate the duplication of data entry. Ensure the telemanagement system is capable of interfacing with other institutional data applications, such as employee ID or project ID databases and accounting feeder files systems.

Wireless Voice

Work with cellular providers to make Berkeley Lab a beta, if not an alpha, site for testing applications. Commit small project funding of about $100,000 from Telephone Services to install microcells in the buildings without cellular coverage. Telephone Services will work with the cellular carrier, most likely AT&T Wireless, to develop an application to interface with the Laboratory's PBX. This will allow users to carry one device for Laboratory phone service, cellular service, PDA, and pager.

Videoconferencing

Provide videoconferencing in at least one large institutional conference room.

Standardize the Laboratory to one desktop videoconference system. Recommend Polycom as the product of choice based on its reliability, user-friendliness, and market share.

File and Printing Services

DESIRED STATE

File and printing services that provide an easy, cost-efficient mechanism for secure and reliable file storage, administration, and print services. File services that are clientless-accessible. Printing services that are available through a client or the Web.

CURRENT STATE

File Services

Laboratory-wide, ITSD-provided file services are based on an extensive Novell infrastructure, which is managed and maintained by the CIS Department. ISS also maintains a component of the Novell infrastructure to support its operations. This environment provides application deployment as well as file storage. CIS also maintains a master NT domain with trust relationships to a number of NT4 resource domains. This does not include corporately managed file services, but does indirectly connect users with files on resource domains through group and user rights. Research into Microsoft Active Directory using Windows 2000 servers was conducted in FY02. Specific areas of research included

- Remote Installation Services (images deployed over the network)
- Application deployment to the computer or to a specific user
- Self-healing of applications
- Security patch distribution

The CIS UNIX group also maintains centrally managed file services using a Network appliance and two Solaris servers. There is also an extensive implementation of Linux and other UNIX-based file services implemented by and for individual groups of users.

Printing Services

Printing is a multifaceted technology problem. Any given printer can be sent jobs through Novell Printing, UNIX Distributed Printing (DP), an NT printer server, or an individual desktop PC, Mac, or UNIX box. The print job can be sent via AppleTalk, IPX (queue-based printing), or IP. The printer itself has an AppleTalk name and zone, a fixed IP address, a Novell print server and printer object or NDPS printer object, and a UNIX DP name. One or none of these might be registered in a DNS resource record.

The UNIX DP system uses AppleTalk as part of the Columbia AppleTalk Protocol (CAP) now used in UNIX distributed printing. UNIX distributed printing does not support the most recent version of PostScript; at present, only PostScript Version 1 is supported. Research into an alternative UNIX printing infrastructure is being conducted by CIS. The Common UNIX Printing System (CUPS) software was written by Easy Software Products, and licensed under the GNU General Public and GNU Library General Public Licenses, and is the main approach being investigated. The test site is comprised of the 40 or so printers in the Earth Sciences Division.

In the past year, a significant effort in the Novell printing environment has resulted in the elimination of AppleTalk as the back-end protocol for sending print jobs from Novell print servers to individual printers. This is now accomplished using IP. Novell Distributed Printing Service (NDPS) is being used to manage Novell-based printing. It does so in two ways: by providing support for old-style queues, and directly through NDPS print objects. At present, some applications (notably the PeopleSoft applications that print through SQR) still use an LPT port redirected to a network queue. This queue could also be serviced by an NDPS printing configuration.

Printer Metrics, as of 7/3/02:

- 496 Novell printers
- 406 DP printers

There are also an unknown number of printers managed by NT4 Resource Domain Print Servers. For example, the Earth Sciences, Environmental Energy Technologies (Energy Analysis Department), and Physical Biosciences (Calvin Lab) Divisions all have NT printer servers.

TECHNOLOGY TRENDS

File Services

Novell

NetWare 6 was recently released. In the future, some portions of the Novell offering (printing via NDPS, directory services via NDS) will continue, along with some elements of NetWare (file system, caching system). Novell, as a company, is still in a transition mode, attempting to compete with Microsoft for the network operating system (file and print service) business as well as gearing up for new applications such as iPrint, iFolders, and Web Folders.

Decision points include:

- ISS application deployment for client/server applications depends on Novell and Netware Application Launcher (NAL). We cannot see eliminating Novell until the client/server is taken over by Web-enabled applications.
- NDS may survive as an alternative to Active Directory on Windows 2000. Active Directory is very weak at the moment.
- Novell is used not only to push the client application to the desktop, but also to manage access to the applications through NDS permissions.
- Start a gradual migration to Windows 2000 Active Directory (AD) in parallel with the existing Novell Directory Service (NDS).

Windows 2000/Active Directory

Microsoft Windows 2000 and Active Directory are the file and print services technologies of the future.

- Active Directory and the “NT Domain” provide workstation security, software deployment, and end-user authentication. Windows 2000 Professional and XP Pro offer increased stability and security over Windows 9x OS's. Both also provide improved centralized client workstation management functionality.

- The time horizon would be driven by compatibility with corporate applications. [Major application software vendors like PeopleSoft and PSDI (Maximo) have not yet certified their applications to be compatible with Microsoft XP Pro. PeopleSoft has a recommended solution for working with Windows 2000 clients that has not yet been implemented at Berkeley Lab.]
- Transition
  - Transfer the (NT) master domain to Active Directory.
  - Modify the legacy client to include LM2 authentication.
- There is general agreement on the following trends:
  - Active Directory is not a prerequisite for adoption of Windows 2000 Professional.
  - Windows XP Pro is the general direction for the client workstation OS over the next two years. Thorough testing must be completed before it is supported as an administrative client OS.
  - Any adoption of Windows XP Pro will require compatibility with the NT4 master domain, Microsoft Active Directory, and (Novell) Netware Directory Services (NDS).

UNIX

Network File System (NFS) Version 3 is used for almost all UNIX filesharing at the Laboratory. Modern UNIX operating systems implement NFS Version 3, which offers acceptable performance over a local area network. NFS is usually used in conjunction with Network Information Services (NIS), which is a directory-type service that facilitates the sharing of a single set of administrative files, such as password, group, and NFS mounted file systems. Currently, there are at least 12 different NIS administrative domains at Berkeley Lab; each is constructed for the purpose of consolidating and simplifying account management across a set of machines in a workgroup or department. The only basic requirement for NFS filesharing is that the users on each participating system must have a unique user ID and login name to avoid namespace collisions.

There is also some limited use of the Andrew File System (AFS) at the Laboratory within the NERSC, Physics, and Nuclear Science Divisions. It has proven well suited for collaborations because it provides acceptable performance across Wide Area Networks (WANS), and offers a more secure and granular method of controlling access by utilizing Kerberos and Access Control Lists (ACLs) for end-user authentication. The original product was commercially licensed through the IBM Transarc Corporation, but it was recently released as OpenAFS to the open source community under the IBM public license. Since it is now free, we may see a renewed interest in adopting its use for some projects.

Printing Services

NDPS is now replacing traditional IPX printing. It can use IPX or IP, and will support UNIX distributed printing. NDPS provides connectivity for most client platforms by supporting the Internet Printing Protocol (IPP) and LPR/LPD. Using open standards allows network administrators all of the ease of managing NDPS printers while still making the printers available to users on a variety of client platforms. NDPS will be used for the next three years.

UNIX Distributed Printing will still be used by UNIX systems managed by CIS. Individual workstations will point to the DP server and a specific printer, and the DP server will handle text translation to a PostScript-capable printer.

UNIX printing could be supported through NDPS. Both LPR/LPD and IPP printing are supported. The key issue will be the support of legacy printing problems like TeX and LaTeX.

UNIX DP will be modernized in the future by moving from the existing CAP-based printing to the Common UNIX Printing System (CUPS) or an equivalent service.

At present, there is no interest in developing a centrally managed print service using the Microsoft Active Directory infrastructure.

There are no current plans to identify and convert Mac systems that print using AppleTalk. However, this should be a consideration going forward.

RECOMMENDATIONS

- An interim objective is to make files on Novell servers available to users via a Web interface (Web folders or iFolder). This will eliminate the need to have a Novell client for this purpose, and will simplify access from offsite locations.
- Create a Microsoft Windows Active Directory (AD) infrastructure for Laboratory-wide use.
- Convert existing NT4 domains to the new AD tree within two years.
- Run Windows AD in parallel with Novell File and Print Services; convert over to AD when appropriate.
- Upgrade the CAP UNIX Distributed Printing Service to CUPS.
- Provide clientless access to file services.

Hardware

DESIRED STATE

Provide state-of-the-art, cost-effective standardized hardware similar to our current desktop and laptop systems to support Berkeley Lab's mission. This includes having the appropriate BOAs for hardware, support contracts with the hardware vendors, spare parts, and internal support services available.

CURRENT STATE

Desktop and PDA Systems

There are no standards for PDA devices, although Palm devices are the most prevalent at the Laboratory. Although Berkeley Lab does not have a standard for PDAs, they are in common use among our staff. They are excellent for schedule, contact, and to-do list management, but are also quickly being recognized as potential mobile communication tools for both data and voice.

A Standard Desktop based on Micron PCs is used for all administrative and some scientific users. There are limited component choices for the Standard, with several choices of monitors.

Although a systems contract with Dell has been established to acquire laptops, the contract has not had a great impact. Most of the laptops bought at the Laboratory are not from Dell, or are not the choices available on the contract Web site. To lower the cost of laptop support, the laptop BOA should be given more consideration. This will assist us with the support of remote users.

There is no standard scientific desktop system. As a result, many national vendors and some local companies provide a wide variety of hardware for the workstation and workgroup server market. IBM, Compaq (DEC), Sun, and Dell are among the national firms, and Fine-Tec is an example of a local firm. Many of the systems are Wintel-based with specialized graphic cards (for example, high-end cards from Matrox), multiple processors, RAID arrays, and expansion slots for use in data acquisition tasks.

Administrative and Infrastructure Systems

ISS hardware implementation employs redundant components to ensure that maximum uptime is achieved. Their system availability is over 99 percent across all of the systems. ISS has separate environments for its production and development systems, allowing for in-depth testing of hardware and software without adversely impacting the production systems. The development and production environments are distributed between two separate buildings, providing a disaster recovery capability.

Infrastructure and corporate applications utilize UNIX servers from Sun for e-mail, LDAP, Web, and calendar services. Network Attached Storage (NAS) is used for UNIX home directories, Oracle database systems, and other corporate data. ISS client-server applications also use Dell servers running NetWare for front-end application service. There is also continued limited use of a vendor owned and operated IBM mainframe for three outsourced administrative applications.

Novell and NT file and print services are deployed using Dell Servers in Building 937 (ISS LAN Operations) and Building 50 (CITG).

Scientific Systems

The NERSC High Performance Computing Facility at Berkeley Lab operates a midrange computer solution called the PDSF, utilizing a large 390-node Linux cluster of PC workstations in a networked configuration. The PDSF is only available to High Energy Physics (HEP) and Nuclear Science users for simulation and data analysis of large-scale investigations.

Berkeley Lab also offers two SMP computer servers (Linux and Solaris) to the Laboratory user community for general scientific use on a recharge basis. The current system is a 64-bit Sun Microsystems Enterprise server running Solaris UNIX. Since many of Laboratory researchers use Sun workstations running Solaris, they are able to easily utilize this computing solution without having to change their working environment or port their software over to a different architecture.

CSAC and ITSD are currently conducting a Laboratory-wide program to raise awareness of midrange computing among Berkeley Lab scientists. The purpose of this is twofold: to determine whether the lack of such an institutional resource is putting Berkeley Lab researchers at a disadvantage in an area that has been identified as a core competency of the Laboratory; and to identify what additional investments, if any, the Laboratory should make in midrange computing capability.

TECHNOLOGY TRENDS

PDA Dev*ic*es

- Wireless synchronization with desktop personal information managers (PIMs; e.g., Netscape Calendar/Addressbook, MS Outlook).

  Example: A user on travel could sync with a calendar server during a meeting to check for conflicts.
- Mobile Internet access.
  - Via PDA/mobile phone, using infrared or cable (e.g., Palm/Nokia 8290).
  - Via PDA with add-on network access device (e.g., Palm/OmniSky, Handspring/GoAmerica Minstrel S).
  - Many modern phones include an internal wireless modem to facilitate data communications.

    Example: Users could leverage their investment in an existing mobile phone to facilitate mobile e-mail, messaging, and Web access.
- Voice/Internet access via PDA with an add-on mobile phone device (e.g., Handspring/VisorPhone).

  Example: Users who don’t wish to carry a phone and PDA can combine them using a modular solution, enabling them to carry just the PDA if they wish.

The technologies described above provide beginning solutions for wireless information exchange, e-mail, and limited Web access. None is yet in a mature state, and standards do not exist for the network or data protocols used to facilitate these technologies. It is reasonable to expect that such standards will be developed in the next two to three years, but it may not be best to evaluate the usefulness of these devices solely based on their connectivity and communications capabilities.

It should be noted that most PDA Web access software only provides good Web access to sites specially designed for lower-bandwidth “smart phone” and PDA connections. This is commonly referred to as “Web clipping.” Users should not expect to access all Web sites using the software/hardware configurations listed above, as some only provide connectivity to specially designed sites.

While many sites are designing “micro-sites” suitable for Web clipping, it is commonly thought that the “killer app” for smart phone/PDA connectivity has yet to arrive. Various financial institutions are announcing solutions for managing accounts and transactions via mobile devices, however, and there are already several companies that distill and distribute news, weather, stocks, etc., for mobile devices. Other applications expected to be appealing are peer-to-peer wireless calendar scheduling (through the network, consulting a server, as opposed to just “beaming” calendar entries), wireless instant messaging, and wireless transmission of electronic business cards.

Berkeley Lab should take advantage of the lack of standardization and current diversity among users and communicate with users of various PDA platforms to find out what works best for them. This communication, combined with more direct research and testing, can provide a useful foundation for making recommendations for the future.

While there may be advantages to specifying a standard PDA platform, it should be noted that more and more emphasis is being placed on interoperability in the PDA arena. The Laboratory should carefully consider the idea of developing interoperability standards rather than platform standards, ensuring that a given device can effectively exchange information with our infrastructure information services, and with a suitably large set of other devices. This will allow the Laboratory to take advantage of the significant benefits of allowing its users to choose which PDA works best for them, while leveraging our investment in existing information management solutions.

The Palm OS is likely to maintain a leadership role in the PDA environment for the next two years.

Some turnkey business applications for inventory control, work order processing, calendar, and note taking are available. MapQuest is a good example of a Web interface to a PDA for quick access to maps and directions.

Laptops/Desktops

Trends in acquiring new computers at Berkeley Lab were analyzed by reviewing data from the Purchasing System. The descriptions on the POs are not always very accurate, which leads to some margin of error. Also, the intended use of some of the x86 systems will be for Linux, but there is no way to know from the description provided. Still, this information does provide some value for the purposes of identifying trends.

Current trends indicate that Apple continues to retain Berkeley Lab market share in the laptop area (over 20%), but that desktop purchases have declined to a level that is more consistent with Apple's overall market share (a little over 6%). With the recent change to Mac OS X, a UNIX BSD-based operating system, these trends could change in the next year or two.

Use of the standard laptop and desktop alternatives made available by basic ordering BOAs declined. It is possible that FY02 figures will change, given the recent improvements made to the online stores for both these vendors

Sony has become a dominant vendor in the laptop area at the expense of Dell.

Purchasing History and Trends:

Laptops	FY99 Percent	FY01 Percent
Dell	40.4	30
Sony	11.4	30
Apple	24.3	21
IBM	9.6	11
Other (Toshiba, Gateway, Compaq, etc)	14.3	8

Desktops	FY99 Percent	FY01 Percent
Dell	20.5	25.3
Micron	44.5	33.5
Apple	23.8	6.2
FineTec*	Not available	18.9
Other (Sun, and a large number of other vendors)	11.2	17.1
*Fine Tec has been the source of custom Linux servers, desktops, and clusters.		

Although progress has been made in developing and marketing a desktop PC standard, it is clear that much more can be done (based on the number of desktop computers that are acquired outside of the BOA).

Standard configurations for desktop machines will continue to be updated. New vendors will be evaluated periodically. The hardware configuration will be reviewed quarterly and changed when required by the vendor or when a technology update is warranted. In any case, the systems will be current, but not necessarily the latest technology. Part of the goal of having a standard hardware configuration is to limit the complexity of maintenance.

There is a need to use incentives to promote the use of standard platforms (e.g., free warranty maintenance for three years). The use of paper controls to alternatives (waiver requests) is not supported by Procurement and is difficult to enforce.

Laptop Issues

- There is a need for more support.
- There is limited use of the laptop BOA, as many other vendor products are also acquired.
- Laptop users have personal criteria for choosing a model (size of keys, type of cursor control, weight, choice of display, and battery life).
- Laptops are much more difficult to configure and update than desktops.
- Remote users have difficulty with setup.
- We need to get some statistics on models users really order and see if we can come up with a better selection and support model for laptops.
- Many companies have docking stations (to connect with large monitors and keyboards) for laptop use at the office.

Servers

There is a trend towards the use of fault-tolerant, scalable systems. In addition, there is a trend towards appliances that have specific targeted functions, like file serving.

Future enterprise class servers, such as those provided from Sun Microsystems, should have the following capabilities:

- Hot swap for processors, I/O, memory, disks, Network interfaces, alternate pathing
- Dynamic reconfiguration of hardware and software changes
- Dynamic system domains (virtual machines carved out of a large resource)
- Storage on the network with cross-platform access and Fibre Channel connections with redundant components and paths
- LAN-free, serverless backups (backup from Fibre Channel switch, which supports a global data store)

Sun Microsystems is a premier vendor of enterprise class servers. However, in some instances, after-sales support has been neither timely nor cost effective.

Workgroup solutions are becoming very inexpensive, which further decreases the need for centrally supplied computer cycles. They do not need to be as robust as an enterprise class server, but should be bought with basic administration tasks (like backups) fully thought out.

Clusters

Cluster technology can be used in the general-purpose corporate computing environment as well as with specialized scientific applications.

A valuable service to the scientific programs would be to assist them in implementing workgroup or small departmental computational systems based on Linux cluster technology. These systems would be more powerful than small workgroup servers and smaller than the Cray T3E and IBM RISC parallel processors envisioned as part of a Laboratory midrange computing resource. Linux clusters are being investigated for use at the Laboratory in collaboration with NERSC's Advanced Systems Group as part of a technology transfer program with the Computing Infrastructure Support (CIS) UNIX Group. There may be some reason to benchmark other open source cluster solutions. The use of Myrinet or 1Gb Backbone solutions for these clusters will be another area of research.

Printers

There is no Laboratory standard or published recommendation for printers. The labor to repair printers has been outsourced.

RECOMMENDATIONS

PDA Devices

- Evaluate interoperability standards and business reasons for extending PDA support within the next two years.
- Consider PDA-based turnkey applications that facilitate inventory control, equipment maintenance, and other activities that require work not performed in an office setting.
- Consider increased use of PDA devices for synchronization with infrastructure applications like calendar and mail.
- Review industry trends for Web clipping applications that allow off-site data sources to be accessed with a PDA device.

Laptops/Desktops

- Promote the use of standard platforms through incentives.

Servers

- Continue to evaluate alternatives to Sun/Solaris as the enterprise platform.

Clusters

- Evaluate and develop support for small workgroup Linux clusters.

Printers

- Publish a list of recommended printers.
- Create an RFP for a printer repair contract that can lower the cost of service to the Laboratory.

Enterprise Networking

DESIRED STATE

- A state-of-the-art, congestion-free Local Area Network (LAN).
- Continued support of Berkeley Lab's scientific goals.
- Keeping pace with Laboratory demand by maintaining and upgrading centralized network services [including the Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP)], as well as LBLnet network-services hardware and software, backbone and building-feed equipment, and basic building distribution hardware.

CURRENT STATE

Overview

Berkeley Lab has become increasingly dependent on its computer network, not only because the network serves an ever-growing number of hosts and servers, but also because other technologies (e.g., environmental monitoring systems and card key readers) now leverage LBLnet to reduce operations costs.

It is clear that continued network utilization growth is inevitable and well justified from a business perspective. For this reason, the maintenance and evolution of LBLnet must be a high priority at Berkeley Lab. The importance of maintaining LBLnet lies in the fact that it serves not only our general computing needs, but also our most visible link to the outside world (www.lbl.gov). Combine this with the Laboratory's mission to encourage open and collaborative scientific research, as well as the multitude of strategic services and applications running over LBLnet, and it becomes evident that the network is a critical resource at Berkeley Lab.

Technologies Comprising LBLnet

LBLnet has been designed and maintained with adherence to the Institute of Electrical and Electronic Engineering (IEEE) and the Internet Engineering Task Force (IETF) standards to ensure interoperability between systems, applications, and Internet connectivity. Any nonstandard implementations in existence are being phased out unless they are essential to research and are the only solutions available. Thus, all nonstandard network services or protocols will eventually be phased out.

See Appendix A for a list of technologies and systems that are used for the general operations of LBLnet.

Equipment and Topology

LBLnet is primarily composed of Cisco high-speed routers and switching hardware. The routers form a high-speed backbone from which over 80 high-speed three-protocol subnets are distributed to buildings in a star topology. These feeds are connected via fiberoptics to in-building Ethernet switches, which are ultimately connected by client hardware (hosts and Ethernet-based equipment). Connections are made via category 3 to 5 (ideally >5) integrated phone and network distribution wiring ideally emanating from a single telecommunications closet. (Many Berkeley Lab buildings either have no telecommunication closets or the ones they have are inadequate.)

Network Services

LBLnet network services, such as the Domain Name Service (DNS) and the Network Time Service (NTP), have current hardware and software. DNS was just upgraded to support Dynamic DNS name updates from a Dynamic Host Configuration Protocol (DHCP) server. This was a major upgrade, and another is not expected in the next five years.

The remainder of LBLnet Services will only require minor upgrades of server and software, ignoring unforeseen impacts of new technologies, such as IPv6. However, as we move closer to an IPV6 rollout, the need for upgrades will become clearer.

Remote Access

Remote access is currently a collage of Remote Access Services (RAS) technologies because of the state of the public telecommunication infrastructure. No single technology provides ubiquitous coverage, i.e., no one technology is available everywhere. Thus, a variety of Internet Service Providers (ISP) must be used to provide coverage for both telecommuters and travelers. Many vendors boast wide coverage, but they are nothing more than multiple ISP front ends. However, Berkeley Lab RAS is supported in-house and is front-ended by a group that provides account administration and vendor-contact support, and that ultimately acts as a single point of contact for LBLnet clients, although this does not address the unique cases where contracted ISPs cannot provide DSL or Cable. Therefore, Berkeley Lab RAS includes in-house support for ISDN and PPP, which provides the Laboratory’s isolated telecommuting or traveling staff (10% of the Lab population) with direct LBLnet access. ISDN and 56Kbps dialup network modems/routers that are maintained in this capacity also provide sporadic research conferences requiring direct connectivity to LBLnet.

TECHNOLOGY TRENDS

Ten-gigabit Ethernet became an IEEE standard in June 2002. The average time from the “Call for Interest” to standard is 2.5 years; thus it is expected that a “Call for Interest” for a 100-gigabit Ethernet will be issued in March 2003, and that standard will be complete in March 2005.

Another relatively new technology, Dense Wave Division Multiplexing (DWDM), allows the use of multiple wavelengths on a single fiber cable. Although DWDM hardware is currently cost prohibitive for use at Berkeley Lab, it may be affordable in the near future as components reach commodity prices. The advantage to using this technology is the ease of increasing bandwidth between points of presence as well as the efficient use of fiber. Since the move of the supercomputing facility from Berkeley to the Oakland Scientific Facility (OSF), there has been an increase in discussion of a high-performance network between the two facilities via “dark fiber” — available fiber that is unused. If the appropriate type of dark fiber can be acquired by either purchase or lease, DWDM would provide a scalable and efficient use of the few strands of fiber.

Currently, there are start-up companies attempting to provide Fiber-To-The-Home. This is gaining momentum as real-estate development companies are considering installing fiber in new housing projects. As such, this could have a significant impact on our ability to provide high-quality remote access and virtual private network (VPN) services.

Handheld Personal Productivity Devices (PPDs) now have wireless support, which will impact LBLnet as Berkeley Lab PPD users demand connectivity to their Laboratory e-mail accounts and other services. Administrative issues, as opposed to technical ones, are likely to present the most significant challenges. For example, there are currently a number of wireless PPD service providers that, if utilized by Laboratory staff, would create a need for centralized billing, which would be problematic due to the various service contracts offered.

RECOMMENDATIONS

To date, LBLnet's router backbone has been upgraded, and the Ethernet switched upgrade is nearing a close. Over the next few years, it will be necessary to replace older in-building switch hardware with more modern equipment. This is necessary to support gigabit building feeds required to maintain uncongested backbone access. This is a multiyear project requiring prioritization of upgrades. The Computing and Communications Services Advisory Committee (CSAC) should be involved in the prioritization of gigabit building feed upgrades.

Project List

- Building Feed Upgrade
  - This will require some new switching hardware.
- Building Switching Hardware Upgrades
  - Not to be confused with the LBLnet Switched Upgrade Project
- Upgrade UPN software

Database Software

DESIRED STATE

All administrative systems are currently using Oracle databases. We foresee no changes in this area for the next 3–5 years.

CURRENT STATE

The Oracle relational database management system is the strategic choice for the Laboratory's institutional applications. Other database management systems, such as FileMaker Pro and MS Access, are in use for smaller, departmental applications.

Relational

- Commercial: Oracle
- Open Source: MySQL, Postgres

Object-Relational

- Future versions of Oracle

TECHNOLOGY TRENDS

Oracle's competitors include Sybase, Informix, and Microsoft SQLServer. Open source alternatives (MySQL, Postgres) are not contenders for corporate business systems, but are being used more frequently in the scientific areas.

RECOMMENDATION

There is no reason to consider a change in the next 3–5 years.

Operating Systems

DESIRED STATE

The Windows desktop operating system (OS) provides support for applications, such as Word, Excel, PowerPoint, e-mail, calendar, IRIS, and LETS, and print and file services that clients need to perform their jobs efficiently. This OS should be well supported, cost effective, reliable, and easy to use.

Server operating systems must support the applications and services that Berkeley Lab requires to perform its mission. They must be scalable, reliable, and easy to manage and maintain.

CURRENT STATE

Windows 2000/XP Pro is the standard OS for administrative systems. IRIX, Solaris, Tru64, and Linux are the supported UNIX variants. However, there is a wide diversity in operating systems in use at the Laboratory, as indicated by the following table.

Microsoft	UNIX	Other
DOS	IRIX	Mac OS 9.x and below
Windows 95	Linux	Mac OS X
Windows 98	AIX	Palm OS
NT4	HPUX	OS/2
Windows 2000/XP Pro	FreeBSD	Netware 4.x, 5.x, 6.x
Windows ME	Solaris	
Windows CE	Tru64 (Dec Alpha OSF1)	

TECHNOLOGY TRENDS

Commercial Operating Systems

The Microsoft Windows operating systems (9x, 2000/XP Pro, and NT) are today’s standard desktops. The operating system for the majority of the desktop clients will be Windows 2000/XP Pro in the future. This will continue to be the operating system that the majority of the Laboratory’s software vendors will support, including both business and office productivity applications. Windows 2000/XP Pro will eventually replace all of the previous versions of Windows and perhaps some of the other operating system clients. The advanced features of Windows 2000/XP Pro include a complete set of usability and systems management features. Some of those features include central software distribution and management; policy definition and enforcement; and security. Other “enterprise” features of Windows 2000/XP Pro include conferencing. Microsoft’s licensing costs are high, and it does not recognize the Laboratory as an institution eligible for educational pricing.

Apple’s Mac OS is prevalent within Berkeley Lab (over 20%), although it is a niche OS worldwide (4.5% of the U.S. market, 3.5% of world market). Macs will continue to be used by some individuals due to personal preference or because of needed functionality. It is expected that the trend in buying Macs will continue to drop. The basis for the new Mac OS X operating system is FreeBSD. It is not clear how aggressive Mac users will be in pursuing an upgrade path, and whether this new operating system will attract users of other flavors of UNIX.

Novell may be phased out over time, with some key components such as NDPS and NDS lasting until other alternatives prove to be better.

Solaris continues to be the premier version of UNIX for enterprise-class applications. Future releases will support:

- Dynamic kernel updates (to avoid reboots)
- OS patches at the routine level with hot fix
- File system snapshots
- A process table that can exceed 32k entries (i.e., up to a million)
- Large directory operations that can support more individual files (e.g., research experiments done with one million files)
- Utilities that can handle terabyte file systems with a much quicker response (e.g., makefs in hours not days)
- Better system management capabilities (i.e., Sun Management Center)

Sun is adding:

- GNOME for the supported graphical user interface (GUI) (and funding the open source development effort)
- Apache, Perl, and many GNU utilities to the standard distribution
- Smart card support
- IP Security Protocol (IPSEC), Kerberos
- Built-in LDAP

The source code for the operating system is open and free to view and use, but the licensing is different from the GNU license in that one cannot develop something using their source code and sell it without first talking to Sun.

Open Source Operating Systems

Open source OS alternatives, such as Linux, FreeBSD, and possibly Solaris should it enter the open source arena, might offer more cost-effective alternatives to Microsoft Windows. However, there are certain issues regarding the viability of open source operating systems:

- Open source is “outside” today’s standard (i.e., Windows and commercial applications like PeopleSoft and Oracle) and is not compatible with it.
- Support is less reliable, since support comes from the public domain.
- Open source often lags behind the adoption of new software features and functions.

- Open source is not as conservative in the release of updates. More aggressive in frequency of changes with less concern about backward compatibility.
- There is less backward software compatibility (to older versions).
- It may not support an enterprise management model with features such as centralized inventory, client workstation administration, or software upgrades.

Advantages and disadvantages of open source include:

- Low cost.
- Support can come from a wide range of sources.
- Some support sources may be “arrogant.”
- The technical and functional direction of the software is not controlled by a commercial vendor seeking to optimize revenue and market share.

Employing open source software in the future does have certain possibilities, although moving to open source as a desktop OS replacement in the short term (one to two years) might be impractical. A two- to four-year time horizon might be more appropriate.

While open source OS alternatives may provide solutions in the future, the Laboratory may not yet be able to employ them as the administrative desktop OS. In the meantime, Laboratory-funded projects could be used to evaluate open source OS hardware and software configurations for both scientific and administrative use.

Linux will be used by the scientists and engineers to run their applications. It will replace legacy UNIX desktop operating systems. Clear evidence of this comes from IBM and Silicon Graphics, both of which are migrating to Linux for their “UNIX-based” offerings. In some cases, researchers will need both Linux and Windows, and the client machines will either dual boot or run both operating systems at the same time using a VMware-type of product.

RECOMMENDATIONS

- It is recommended that UNIX support be restricted to Solaris and Linux in three years. Solaris will continue to be used on high-availability, enterprise-class machines. Linux will assume the predominant role in UNIX desktop, workgroup servers, and cluster configurations.
- Certify and implement Windows 2000 for all business applications as an administrative system for Financial Management System (FMS) users.
- Support Mac OS 9 for one more year through FY03.
- Continue to evaluate Mac OS X.

Desktop Software

DESIRED STATE

- Alternatives to Microsoft Office are available for customers who use Linux/UNIX platforms.
- Standardized use of a smaller number of desktop applications, such as HTML-editing software.
- Offering a better life-cycle support (such as training, consulting, troubleshooting) for each desktop application.
- Selections of software products to support in the future (through centrally provided acquisition, training, or the Help Desk) are based on Laboratory needs and functionality.

CURRENT STATE

Some inefficiency in desktop software support occurs because of the wide range of tools used by Berkeley Lab customers. It is very difficult to provide high-quality Help Desk and Mac/PC support if there is no standardization in what customers use.

Berkeley Lab is a research laboratory with a diverse set of computing requirements, including a substantial base of UNIX/Linux users. There is a need to interchange documents between researchers and our administrative staff. Alternatives to the Microsoft Product Suite, which is the standard for Windows and Macintosh desktops, need to be investigated [particularly for documents such as Performance Review and Development (PRD) forms that have a Laboratory-wide scope].

Selections of software products to support (through centrally provided acquisition, training, or the Help Desk) are based on functionality and Laboratory needs.

The following table documents commonly used desktop software:

Desktop	Utilities	Scientific
MS Office	TechTools	
MS Project	Norton Utilities	Mathematica
MS Access	Norton AntiVirus	Ghostscript/ Ghostview
MS FrontPage	DAVE (Mac utility used to access windows filesharing)*	SPSS 10
MS PhotoEditor		LabView
Adobe Photoshop	StuffIt (similar to Winzip)	PowerCADD
Adobe Illustrator	SSH	AutoCAD**
Adobe InDesign	BBEdit (editor)*	Mathcad
Adobe Acrobat	Textures*	Origin
Adobe GoLive	Eudora (mail client)	
Macromedia Fireworks		
Macromedia Flash	Connected Backup	

Desktop	Utilities	Scientific
FileMaker	WinZip	
Canvas (2d drawing)	Exceed (Xterminal emulator)**	
Macromedia Dreamweaver	WS_FTP	
Claris Homepage	Crisp (ISS text editor)	
Adobe Pagemaker	PC NFS	
QuarkXpress	Timbuktu	
Framemaker	VNC	
Visio		
Pagespinner*		
Netobjects		
StarOffice		
RFFlow		
PMDiff		
Helios Textpad		

* Mac only

** Windows only

TECHNOLOGY TRENDS

The recommended support strategies for standard software are shown in the following table. (Note: "Aggregation" means that the license is acquired by virtue of buying a standard PC, which comes with licenses for the operating system and desktop software, or the license is acquired via a central buying service.)

Product	Standard Load	On-site Training	Help Desk Support	License Support		
				Site	Volume	Aggregation
Desktop						
MS Office	X	X	X			X
MS Project						X
MS Access	X	X				X
Adobe Photoshop		X				
Adobe Illustrator		X				
Adobe Acrobat		X	X			
Macromedia Dreamweaver		X	X		X	
Visio		X				X
Open Office/StarOffice		X	X	X		
Utilities						
Norton AntiVirus	X		X	X		
WinZip	X		X	X		
WMware			X		X	
DiskKeeper						X

Product	Standard Load	On-site Training	Help Desk Support	License Support		
				Site	Volume	Aggregation
Remote Workstation Access and Control						
VNC (free)			X			
Timbuktu (100 licenses)			X		X	
WinXP Pro built in remote control						X
Terminal and File Access						
Exceed					X	
SSH	X		X	X		
WinSCP						
NFS (Mystro)						
Scientific						
LabView					X	

RECOMMENDATIONS

- Evaluate StarOffice as an alternative to the Microsoft Office Suite.
- Support Dreamweaver as the corporate Web page development package.

Workgroup Collaboration

DESIRED STATE

A digital workplace for accomplishing day-to-day work at Berkeley Lab that is used by cross-functional teams to plan, execute, and control projects or implement new processes. Our desired state includes workflow and conferencing functions.

Workgroup collaboration is characterized by the following:

- Integration with existing directory services for a list of potential contributors and authentication services (e.g., LDAP)
- On-line anytime, anywhere access via the Web
- Knowledge base (white papers, checklists, requirements analysis, discussion threads, small databases)
- Digital collaboration tools (whiteboard, real-time chat services, conferencing and presentations, routing and tracking mechanisms)
- Project management and control (tracking of tasks and milestones, progress reporting, shared calendar, version control on key documents)
- Decision-making processes (surveys, voting/polling methods, multistep approval mechanisms)

There are two types of collaboration tools:

- Static collaboration tools that allow team members to share documents, have threaded conversations, maintain a project calendar with milestones and tasks, vote, and maintain a common view on project status.
- Dynamic collaboration tools that allow real time conferences (Video and Audio) or, in some cases, sharing via an instant messenger type of application. Share documents in real time via white board application.

CURRENT STATE

At present, there is no corporate solution for workgroup collaboration. Individual groups have experimented with the concept (e.g., the Energy Analysis Department in the Environmental Energy Technologies Division uses QuickPlace from Lotus for this purpose). Informal solutions to collaboration have been implemented using shared directories on file servers, access to documents via the Web, and through extensive use of electronic mail to exchange documents. However, this does not provide workflow control or version control of documents.

TECHNOLOGY TRENDS

Three products have been identified as evaluation candidates to date:

- QuickPlace from Lotus (evaluated in Spring 2002)
- eRoom (Summer 2002)
- Novell Workspace (TBD)

RECOMMENDATIONS

- Evaluate tools that would provide workflow and collaboration support, and the need for these tools.
- Select one or more pilot projects, identify costs and benefits, and recommend future approach.

Security

This section discusses security considerations at Berkeley Lab. The goal of the Computer Protection Program (CPP) is to protect Berkeley Lab computer resources from security-related occurrences that detract from the Laboratory mission. To this end, the CPP attempts to provide protection, but not to the point of interfering with important scientific and other computing activities.

DESIRED STATE

Computing and networking resources are protected by industry-standard security technology, such as firewalls, screening routers, antivirus software, third-party authentication, and intrusion detection, so that they have integrity and are reliable. Firewalls and screening routers, for example, can block incoming attacks that might otherwise change the integrity of systems and network devices, or cause denial of service. Antivirus software keeps systems from becoming infected with viruses and worms, something that causes downtime for users. Third-party authentication helps ensure that only authorized users can access systems and networks; in doing so, third-party authentication helps ensure system and network integrity in addition to availability. Intrusion detection is an indirect protection measure in that it is necessarily a post hoc mechanism. Intrusion detection nevertheless enables security and technical staff to quickly identify how and where security has been breached, helping prevent further damage and disruption.

CURRENT STATE

Overview of Berkeley Lab's Security Strategy

Intrusion detection and host-based security form the main basis of Berkeley Lab's security strategy. A spam and antivirus wall blocks spam traffic and most viruses, worms, and Trojan horse programs contained in messages. Packet filtering based on ACLs is used by routers at external gateways, and has also been installed for the corporate Information Systems and Services (ISS) servers. Security is additionally built into standard installations and maintenance procedures used by groups such as the Mac/PC Support Group. Because ISS has systems and data that process and store financial, personal, and other sensitive information, ISS has deployed additional protection measures, such as a firewall, and encrypted sessions for accessing critical applications, such as LETS. The CPP and others also periodically identify important issues (such as cleartext logins) and develop solutions for them.

Detection

Berkeley Lab's intrusion detection capabilities are based on a Laboratory-developed intrusion detection system (IDS) named "Bro." Bro is different from (and thus in many ways superior to) most other IDSs in that it is not reliant on attack signatures per se, but is based on rules that incorporate sophisticated logic conditions. Rules include some signatures, but also are more often based on how normal the behavior of network protocols is, the types of connections in and out of Berkeley Lab's internal networks, the nature of outbound connections, references to Trojan horse programs in user command entry, and other indicators of attacks. Bro can also dynamically block IP addresses based on observed traffic, “shunning” incoming connections from source IP addresses that it determines have launched attacks against Berkeley Lab systems.

Bro has served Berkeley Lab well, but numerous concerns about Bro need to be addressed. Bro intrusion detection is, for example, oriented towards detecting attacks against UNIX but not Windows machines, even though Windows machines are now more prevalent at Berkeley Lab. Bro operations, particularly troubleshooting and system management of Bro boxes, also tend to be labor intensive. Additionally, Bro was originally developed as a research project; thus, it was not subjected to software engineering methodology. Bro documentation is consequently incomplete and not always accurate. The one thread that holds Bro and its operations together is its developer, who now works as a full-time employee for another organization, and thus can work for Berkeley Lab only four hours per week. If sometime in the future this person should not be available to Berkeley Lab at all, the future of Bro would be severely jeopardized. Finally, the utility of “shunning” is becoming questionable because of the amount of attacks in which packets have spoofed IP addresses, and also because shunning causes the filtering rules in routers to fail for a few seconds, temporarily leaving the internal network exposed to attacks that would normally be blocked.

Some of the concerns about Bro are already being actively addressed. Several efforts to improve and upgrade Bro are currently underway. One such effort, for example, is aimed at reducing the time it takes to change router ACLs. Additionally, funding from DOE to improve and advance Bro’s capabilities has been requested.

Host Security

Host security is achieved through a number of methods. The CPP has created protection guidelines for the major operating systems used at Berkeley Lab, and has posted them on its Web site (www.lbl.gov/ITSD/Security/guidelines/). The CPP also often holds courses on securing operating systems at Berkeley Lab, and encourages system administrators and others to take outside courses, such as System Administration, Networking, and Security (SANS) courses on UNIX, and Windows systems security. Most significantly, however, the CPP has initiated an ongoing vulnerability-scanning program in which Berkeley Lab hosts are scanned (normally once a month, but more often if a new high-threat vulnerability emerges). The owners and/or system administrators of any systems found to be vulnerable are contacted and asked to fix the vulnerability. After several requests, if a system is still vulnerable, that system’s IP address is blocked from Internet access. The percentage of compliance has been very high so far, resulting in very few systems with dangerous vulnerabilities. Proof of the effectiveness of the vulnerability-scanning program is the fact that during the second quarter of 2002, there were almost no successful break-ins to Berkeley Lab systems, despite a vast number of attempts.

Remediation

Remediation occurs in a variety of ways. Most of the patches are applied manually, with no automatic distribution of security patches to Windows clients at all, and very little in the way of timely updates because the vast majority of systems are not under any kind of management contract. UNIX systems that are managed (these include approximately 250 systems) get timely patches, but this process is not fully automated, although scripts are used.

The same is for the most part true of Windows systems. The first use of Windows NT domains grew out of the user community. The ad hoc appearance of Windows NT, the fragmented evolution of the master accounts domain now managed by the Computing Infrastructure Technology Group (CITG), and the many resource domains managed by individual divisions have resulted in security vulnerabilities due to the widespread implementation of shared network accounts, file and directory sharing, printer sharing, and Web services. Berkeley Lab is migrating to a single-domain native-mode Windows 2000 Active Directory implementation. Doing so can potentially be advantageous to Windows security, because Domain Administrators can perform central security administration that allows efficient push-outs of Service Packs and hot fixes. Central security administration is also likely to result in better configuration and policy settings than those set by individual administrators. At the same time, however, Active Directory is very complex to manage, and some remote administration methods are based on less than ideal methods[1] from a security viewpoint.

Macintosh systems are, however, in a class by themselves. Relatively few of these systems are managed by a system administration group; security in these systems tends to be very lax. Fortunately, Macintoshes have fewer security-specific threats than the other operating systems used within Berkeley Lab.

Virus and Spam Protection

Both a spam wall and a virus wall are maintained on the corporate incoming mail servers (postal1 and postal2). The virus wall, for which signatures are constantly updated, prevents a large number of virus infections every month, but does not protect systems that receive mail through a mail server other than the ones that link to the virus wall. The Laboratory has purchased a site license of Norton AntiVirus software; this license also allows installation of this software on users' personal systems.

Router-Based Security

Routers at the entrance to the LBLnet, ESnet, and National Energy Research Scientific Computing Center (NERSC) networks have ACLs that block certain types of potentially dangerous traffic. For example, with the exception of IP source addresses in NERSC's network, all traffic bound for User Datagram Protocol (UDP) ports 137 and 138 is currently blocked to protect Windows systems from certain kinds of attacks. It may be necessary to block additional selected types of network traffic to further increase security of Windows and other environments. The ACLs are not very restrictive, however, because of the diverse access needs of the Berkeley Lab scientific community.

Desktop Security

Desktop security is difficult to achieve, in large part because desktop operating systems generally have fewer security capabilities than do operating systems intended for servers. There are hundreds of Windows 95/98 machines and Macintoshes that have little security. In addition,

[1] The Active Directory-based Remote Installation Service (RIS) requires, for instance, that the Windows Installer service run on every system that RIS reaches.

in the past it was common to have users open file shares that allowed anyone to read or write to their systems' hard drives with no requirement for even a password. The CPP's vulnerability scanning effort has resulted in identification of these systems, whose owners were contacted and asked to either delete these shares altogether or otherwise restrict access to them. As a result of this effort, there are presently almost no Berkeley Lab systems with unprotected shares. Another concern is that the antivirus software, which runs on many systems, is not adequately updated as new viruses and worms emerge. The Information Technologies and Services Group has developed a method of pushing antivirus software updates to desktop systems; this method is currently being deployed with less than 100 systems, with the intention that the number of systems that receive automatic updates will grow in time.

To the maximum extent possible, all desktop machines will conform to a standard security profile. This can be installed during the initial load, or in special cases, manually installed after the system is configured for use. Windows 9X, 2000, and XP Pro workstations will be maintained by electronically updating patches and making required configuration changes. In order for the automated security management to function, a domain or Windows 2000 Active Directory will be necessary. All Windows client machines will need to be members of this domain or directory.

Improvements in desktop security (securing open ports, disallowing shares with access to everyone) can be made by the implementation of personal firewall software, and by correctly using the NT File System (NTFS) permissions built into NT4, Windows 2000, and Windows XP Pro file systems. These improvements will be part of the standard load.

Server Security

The main concern about server security is the diverse configuration and deployment methods used for servers. Many servers are installed and maintained by one of a number of groups that provide system administration services. These servers tend to be more secure than others because technical staff from system administration services usually understand security issues and solutions reasonably well. Patches and upgrades are more likely to be installed in these systems. The worst cases are systems installed by individuals who do not know very much about security. Many of these systems become "orphan systems" — systems that are not maintained. Orphan systems are in many ways a worst-case scenario for security in that not only do they have a high risk of being compromised, but they also are "weak links" that serve as intermediate points for attackers who, once they have access to an orphan system, can attack other systems within the Berkeley Lab networks more readily. Orphan systems need to be identified and measures put in place to ensure that at least some minimal amount of effort is invested in securing and maintaining these systems. A long-term goal is the use of strong authentication methods, such as smart card-, Secure ID-, or biometric-based methods, to identify users. This authentication will eventually be integrated with other systems that provide a single sign-on capability.

Public Web and File Transfer Protocol (FTP) servers at Berkeley Lab are also a special concern. The best way to deploy public servers from a security perspective is on a demilitarized zone (DMZ)[2], but doing so is not at all feasible at Berkeley Lab. Anyone on the Internet can thus get inside the Laboratory's network to reach Web and FTP servers. Once anyone (or any malicious program) gains access to a server, Bro may not be able to determine subsequent actions on the part of the user or program because it is a perimeter-based IDS. The best solution so far has been to inventory the Web and FTP servers used at Berkeley Lab, and to periodically scan them as part of the scanning effort described previously in this section.

Application Security

To date, relatively little attention has been paid to application security. Web-based applications are a particular concern because of the ease with which Web servers can be accessed from virtually anywhere in the world, and also because of the difficulty of writing secure Web applications. A project is underway to implement a standard authentication system for in-house-developed Web applications. This authentication system will be available to any application that uses Lightweight Directory Access Protocol (LDAP) to identify valid users. Common routines are being written for interface to applications written in Perl, ASP, and JSP. Once this solution is in place, Laboratory employees will have a single sign-on service from Human Resources Self-Service; Environment, Health and Safety (EH&S) sites; the IRIS Data Warehouse; and other ITSD-developed Web applications.

Data Communications

There is extensive use of telnet and FTP, both of which allow cleartext transfer of user IDs and passwords. Secure Shell (SSH) software is, however, becoming more prevalent within the Berkeley Lab user community, and is also being used for corporate applications such as LETS and Oracle Purchasing. On servers and workstations, SSH Version 2 is available. Version 2 for servers allows for downward compatibility and support for SSH Version 1 clients. There is currently no standard for secure file transfer. A workaround for secure file transfer is to enable SSH Version 2 at the client, and to install SSH Version 2, with Version 1 compatibility enabled on Laboratory servers. The CPP also recommends the use of a freeware secure file transfer program (SCP) for UNIX and Linux platforms, and WinSCP for Windows platforms.

Recently, SSH has been deployed for access to business-sensitive systems, such as LETS and Oracle Purchasing. This is not a solution that has been overwhelmingly adopted, however. Telnet is still used, and as a result, user IDs and passwords are passed in clear text. FTP is still used to copy files in a cleartext mode as well. ISS needs to move towards full adoption of SSH and a Secure Copy protocol.

The Laboratory has an IP-based Virtual Private Network (VPN) managed by the Network Services Group. More recently, Berkeley Lab has procured Personal Ravlin II VPN appliances and several Red Creek VPN servers, and has begun to push the appliances out to the Laboratory user community with the goal of providing more efficient and secure tunneled links from offsite locations to LBLnet.

[2] A DMZ is a network segment on the external gateway, not within the internal network, that is afforded less protection than internal systems, but which, if compromised, will not serve as much of a threat to internal systems because it is not within the internal network.

Offsite access to Laboratory data is frequently accomplished by using remote control products, such as Timbuktu and Virtual Network Computing (VNC). Remote control products as a whole are beset with security problems, the worst of which is the unauthorized use of these products to gain control over virtually any system that has a Timbuktu or VNC client. The fact that apparently no incident involving unauthorized access via a remote control product has occurred so far, however, diminishes the magnitude of concern that needs to be devoted to this issue.

The CPP is also attempting to get telnet and rlogin services turned off when the UNIX Support Group installs new UNIX systems. The CPP has also initiated training and awareness efforts to make the user community aware of the dangers of cleartext logins.

Wireless Networks

A final area of concern at the Laboratory is wireless networks. The demand for access via wireless networks is rapidly growing. Anyone within the transmission range of a wireless transmitter can potentially connect to a wireless network, and also can possibly steal network communications. Although the Networking Group is supposed to install and maintain all wireless networks at the Laboratory, rogue transmitters have already been identified. The CPP is currently studying the implications of the growing use of wireless networks at the Laboratory, but has not yet taken any action to deal with this issue.

TECHNOLOGY TRENDS

Trends that are likely to impact or enhance services at Berkeley Lab include the use of staging servers for making updates, the deployment of third-party authentication solutions, the increasing capabilities of IDSs and the growing use of these systems, and the deployment of security-related measures in wireless networks.

Staging Servers

Staging servers, which can be used to push updates (patches, antivirus software, and so forth) to remote systems, are not only efficient in terms of manpower requirements, but also virtually guarantee that changes that need to be made for security's sake are indeed made. Staging servers, already in limited use at Berkeley Lab, promise to reduce the number of security-related incidents below the current number (which is already small).

Third-Party Authentication

Third-party authentication is gaining acceptance and use. In particular, smart cards (computer chips embedded in laminated cards), token generators, which generate a challenge string entered by the user, and biometrics (e.g., authentication based on fingerprints, retinal scans, and/or facial shape), are increasing in use, especially in government and banking organizations. Using third-party authentication would not only reduce the number of security-related incidents, but it would also eliminate the need for passwords. Passwords are badly outdated and pose many security-related dangers to the Laboratory's computer and networks because they are guessable, accessible (often because users write them down), and sharable. Eliminating passwords in favor of using third-party authentication would also greatly reduce the workload of the Berkeley Lab Help Desk and system administrators, resulting in substantial monetary savings. It would be relatively easy to embed smart-card chips in Berkeley Lab employees' badges.

Intrusion Detection Systems (IDSs)

Another trend developing in the computer security industry is the increased performance and capabilities of IDSs. Effective intrusion detection enables technical staff to intervene quickly when incidents occur, reducing the resulting impact and costs. IDSs are becoming increasingly faster; several vendors claim to have developed IDSs that can perform full intrusion detection analysis at network throughput rates of up to 1 gigabit per second (GbS). Additionally, several new IDSs not only detect attacks, but also stop packets that are sent in connection with an attack from reaching their destination. Although Berkeley Lab has its own intrusion detection technology, deploying other IDSs on at least a limited basis would substantially increase the Laboratory's intrusion detection capability.

Wireless Network Security

Wireless networks pose many security threats, but many security measures have become available over the last few years. Encryption of wireless communications is the most important new trend. Encrypting wireless communications prevents hostile parties from capturing the content of these communications to glean passwords, data, and other information. Additionally, wireless networks are increasingly incorporating mechanisms that require the Media Access Control (MAC) address of each user's system for access authentication. This technology trend is potentially important to Berkeley Lab because the demand for and use of wireless networks at the Laboratory are rapidly increasing. Implementing appropriate protection measures will greatly decrease the risk of "drive-bys" — capturing wireless communications in one's physical vicinity. It will also substantially reduce the possibility of unauthorized access to Berkeley Lab networks through unprotected wireless networks.

RECOMMENDATIONS

- Systematically investigate, test, and implement supplemental IDSs to address Bro's limitations. Implementation will address redundancy and reliability, speed improvements, detection of Windows and UDP attacks, and documentation.
- Continue the present vulnerability scanning program as it is.
- Develop a strategy for desktop security on Windows platforms, in particular, expanding the number of desktop systems for which antivirus software and security-related fixes are automatically updated.
- Promote the use of service-level agreements (SLAs) involving system administration by experienced technical staff. Standard rollout and maintenance procedures and also the use of centralized back-up services need to be part of SLAs.
- Examine and test third-party authentication technologies.

- Develop a strategy for systematically eliminating cleartext logons and sessions, regardless of the particular protocol used.

Business Software Development and Deployment

DESIRED STATE

The goal of ITSD is to acquire commercial software packages to meet or exceed best business practices, and to modify our business practices to follow the functionality of the application. In-house developed applications utilize JSP and Java as languages to deliver thin-client Web-deployable applications.

CURRENT STATE

Software Development Environment

Overview

There are several different choices that can be made for Web application programming. They are influenced by trends in the languages and tools made available by companies such as Sun and Microsoft, and the target platforms for each product.

The goal is to develop software that supports a thin-client, Web-based model.

Applications have been developed using the following tools:

- Client: thin user interface (server-driven UI) or thick user interface (client-driven UI)
- Development tools: Microsoft model, Sun Java-based model, Perl/CGI model, or other
- Stand-alone development environment: languages or Integrated Development Environments (IDEs)

The Sun solution is characterized by the use of Java, JavaScript, client-side applets, server-side servlets, JSP, and Java Beans. There is currently limited CIS/ISS expertise with most of these tools.

The Microsoft solution is characterized by the use of Visual Basic, VBScript, JScript, ASP, and COM objects. ISS Web application development uses these tools extensively at the present time. It is being extended with the development of the .NET initiative, but there is still very little information available to the public.

A third alternative involves the use of Perl CGI scripts and the CGI-BIN structure to develop and deploy Web applications, along with some use of browser-side scripting languages. There are an increasing number of object-oriented modules in Perl, wide support for the language, and expertise readily available within CIS and ISS. For example, IRIS uses the Perl model. In addition, PHP is being used as an ASP/JSP type of component facility within the Perl community.

All three solutions include the use of HTML, some form of browser-side scripting language, and, in the future, XML.

Thin versus Thick Clients

Thick Client

The thick-client approach requires that a Java Virtual Machine (JVM) be available on the client, either as part of the browser or as a third-party product (JInitiator for Oracle/WebLETS, for example). The JVM interprets bytecodes that simulate a machine language. The translation to the native operating system is made when the application is invoked. An applet is downloaded to the client machine, and it is interpreted by the JVM.

This approach takes bandwidth on the network, and is responsible for an initial delay. Although there is nothing inherent in the product that requires interpretation of the bytecode file (rather than a one-time compilation, as deployed today), each invocation of the application requires a repeat of the same process.

Using a thick client also establishes the need for client-side operating system support, and makes the relationship between the desktop operating system and the application more dependent.

Oracle is retaining the heavy-client Java running on a certified JVM as part of its Oracle Developer strategy. The JVM is JInitiator.

This model is an expensive way to deploy an application, as each client requires the following configurations: JVM installation, Windows registry maintenance, and JVM updates. Running client-side Java requires transferring the entire application to the client at runtime (minimum 1.2 MB of data just for the Java class files required for Forms), making deployment undesirable over a dialup connection.

However, Oracle does support the use of JDeveloper, a Java development environment that is based on Borland’s JBuilder.

Thin Client

The thin-client methodology also provides for a scripting language like JavaScript in Netscape (JScript in Internet Explorer). It is quicker and less dependent on a particular desktop operating system than a thick client, and requires no download configuration.

XML

The HTML standard is now at Version 4.01. The World Wide Web consortium plans to move towards Version 1.0 of XHTML rather than to continue to advance the HTML standard. XHTML is based on the concepts of XML. XML is described as a “meta-language for describing markup languages. In other words, XML provides a facility to define tags and the structural relationships between them [whereby all] of the semantics of an XML document will either be defined by the applications that process them or by stylesheets.” (Norman Walsh, xml.com)

Sun Microsystems Architecture

Sun provides a software tool set that primarily runs on UNIX systems, but is increasingly cross platform.

For client-side, browser-based scripting, JavaScript is provided.

Java is the principal theme of Sun's architecture. Java is used to develop servlets running on a Web server, and applets that are run on a thick client by a JVM. Servlets are Java technology's answer to CGI programming.

Microsoft's Architecture

The typical Microsoft implementation today requires the use of the NT-based IIS Web server, the use of ASP, and some level of browser scripting. It is used heavily for rapid application development because of the availability of components that allow local developers to make use of functionality they would otherwise have to develop themselves.

.NET is Microsoft's answer to Sun's J2EE environment. It includes a new language (C#), a common language format that produces a bytecode file run by a client-side runtime environment, a set of components accessible from the client environment, and support for ASP compiled into the common runtime environment from a variety of languages. It also includes a user interface component on the client side and a new generation of data-access components. .NET is a future consideration, but is likely to be a Microsoft-only solution, requiring a commitment to Microsoft products.

Perl/CGI Architecture

The Perl/CGI model is cross platform. Web servers reference independent programs in the CGI-bin directory, which invokes a separate process for each invocation (HTTP request). Client-side scripting within the browser provides thin client support. There is extensive use of this technology at Berkeley Lab. Perl modules can avoid a great deal of programming, and there is a wide-open source support for these components. Both the IRISv2 and HR Self-Service applications are examples of enterprise applications written using Perl.

Application Development Software

A variety of software-development tools are used, including Oracle Developer, Visual Basic, Perl, JavaScript, and ASP for in-house-developed applications, and PeopleSoft and MRO for third-party vendor-provided applications.

Current institutional applications (including PeopleSoft Financials and HR, Grants, Purchasing, Accounts Payable, and MRO Maximo) employ a client-server model with Microsoft Windows as the desktop OS. Both of these third-party software vendors have Web-enabled versions of their software. This technology direction would reduce our reliance on Windows desktops.

Oracle delivers forms/reports applications to the Web using their forms/reports server as a "black box" that accepts a client-server binary and reproduces a form/report in Java code. Executing the Java code requires a JVM on the client platform, so the form/report can be run on any platform that has a JVM meeting a Sun Java specification supported by Oracle.

A JVM can be built into the browser and use the browser's windowing environment, or can be used as a standalone program that provides its own windowing environment. As of now, we can deploy on the PC using Oracle's JVM (JInitiator), and on the Mac using Apple's JVM — the Macintosh Runtime for Java (MRJ). JInitiator is a debugged version of Sun's JVM, and is distributed as a plug-in to Netscape and IE using HTML designed to force the browser to use the plug-in JVM rather than its own built-in JVM.

Oracle intends to move away from client/server runtime engine in Forms 7, but Oracle is concerned it will lose customers so it has announced continued support of Forms 6i through 2006.

SQR, Actuate, Crystal Reports, PeopleTools, and Oracle Report Writer are all used to deliver reports.

Development Tools

Software tools can be categorized as follows:

- Enterprise: For large user-base and high-transaction volume applications.
- Rapid Application Development: For a smaller number of users and transactions.
- Personal and Workgroup: Typically employed by the end user, and not by Information Systems and Services/Computing Infrastructure Support (ISS/CIS).

This table describes the products included in the ISS/CIS toolset:

Product	Enterprise	Rapid Application Development	Personal and Workgroup	Recommendation
Languages				
C	x			As Required
C++				Not Used
C#	x			Defer (Consider as Part of .NET Initiative)
Java	x			Evaluate
Visual Basic	x			Reevaluate in Future
Perl	x	x		Recommended
PHP	x	x		
PLSQL	x			Recommended
SQLPlus				
JavaScript	x	x		Recommended
JScript	x	x		Evaluate for IE
VBScript	x	x		Phase Out for Client Server Apps
XML	x			Recommended
Microsoft ASP/COM				Reevaluate
.NET				Evaluate
JSP components	x			Recommended
Javabeans	x			Evaluate
Application Development Packages				
JDeveloper, JBuilder, others				Evaluate for JSP IDE
Oracle Developer	x			Reevaluate in Future
PeopleTools from PeopleSoft	x			Recommended

Product	Enterprise	Rapid Application Development	Personal and Workgroup	Recommendation
Web Page Development packages				
Dreamweaver	x	x		Recommended
Frontpage			x	Phase Out
Macromedia Homesite		x	x	Recommended
Net Objects				Phase Out
Cold Fusion				Phase Out
Report Writers				
Crystal Reports	x	x		Recommended
Oracle Report writer	x			Recommended
SQR (from Scribe)	x	x		Recommended
SQLPlus	x			
Actuate			x	Recommended
Database Packages				
Oracle	x	x		Recommended
SQLServer		x		Phase Out
Postgres, MySQL		x		Evaluate
FileMaker pro		x	x	Phase Out
MS Access			x	Recommended
Software Modeling				
Rational Suite (object oriented)	x			Evaluate
Data Modeling				
Visio Professional		x	x	
Oracle Designer	x			
Version Control				
PVCS[1]	x			Recommended
Stat (for PeopleSoft)	x			Recommended
RCS (free on UNIX)				Phase out
Production Control				
Maestro	x			Recommended
Shell Scripting Languages				
Bourne				
Korn				Recommended
C				

[1] PVCS is implemented as the version control tool for all business applications.

Note: Java is supported on a cross-platform basis: Microsoft Windows 98, NT 4.0, Sun Solaris, and Linux (Red Hat 6, Mandrake 7.0). Note that the Java products are certified for these platforms, but also work on others. Apple Mac OS X will be supported following the Mac OS X general release.

Recommendations should be based on the following criteria:

- Market penetration
- Vendor stability
- Security
- Maintainability
- Scalability

Business Applications

Our institutional business applications include the following:

- Vendor Provided
  - PeopleSoft Human Resource Information System (HRIS)
  - PeopleSoft FMS
  - MRO (Maximo)
  - Purchasing and Receiving (PeopleSoft Purchasing System)
  - Requisitioning System (PeopleSoft eProcurement System)
  - Sunflower Property Management System (Annams)
  - Ohm (Health Services software)
  - Restrac Resume Reader (Webhire)
  - Remedy Help Desk Software (Remedy Corporation)
  - Comprehensive Tracking System (CTS)
  - Card-key system (Casi-Rusco)
  - Program Management and Tracking System (PMTS), supported by Oak Ridge
  - Accounts Payable and Travel Disbursement System (PeopleSoft Payables)
- In-House Development (Legacy)
  - Procurement Card (purchasing software originally acquired from LLNL but supported locally)
  - Systems Contract
  - Federal Express
  - Sponsored Proposal and Project Tracking System [IBM mainframe system, outsourced to Acxiom, will be replaced by RAPID (PeopleSoft Grants System) in late 2002]
  - Travel Accounting System (IBM mainframe system, outsourced to Acxiom, will be replaced by Gelco Travel Manager in late 2002)
- In-House Development (Recent/New)
  - IRISv2 (Data Warehouse and reporting system)
  - Lets/WebLETS (timekeeping)
  - Janus (planning system)
  - JHQ (EHS training management system)

  - SHOEBOX (Hazardous Waste Tracking System) developed using Oracle Developer
  - TELEMETRY System
  - Odyssey (a space allocation and recharge system developed using Oracle Developer)
  - HR Self-Service
  - Labor Distribution
  - Current Job Opportunities (CJO)
  - Web Job Order (for Engineering)
  - Signature Authorization System (SAS)
  - Hazards, Equipment, Authorization and Review (HEAR) Database
  - Web-based Radiation Exposure Monitoring System (REMS)
  - Web-based Chemical Inventory Management System
  - Web-based Supervisor Accident Analysis Reporting System (SAAR)
  - Web-based Radiation Authorization Tracking System (RADAR) — upgrade in progress

- External Interfaces
  - BCS — Benefits
  - UCRS — Retirement
  - IVR — Bencom
  - Benefit Carrier Enrollments
  - Purchasing Interfaces for System Contracts
  - VWR (Boise), GC Micro, Granger, Sigma-Aldrich Company

Application Deployment

Software Deployment Technologies include:

Technology	Where Used
NAL (Netware Application Launcher – Zenworks 3)	Client/Server [FMS, HRIS, Janus (application and SQLNet on client, database on server)]
Tivoli	Monitoring of UNIX systems
Microsoft SMS	Not used
Microsoft Active Directory	To be tested: Desktop software, OS service packs, and security patches.
Web browser, thin client	Three-tier, thin Web client (IRIS, using JavaScript and HTML on the client end, Perl CGI on server side)
Web browser, thick client	WebLETS, using JInitiator for the JVM
Manual method	Desktop software when not part of the standard load

Desktop Software Management and Deployment Tools can have the following capabilities:

- Software Distribution
- Inventory
- User administration
- Distributed monitoring
- Security
- Directory services
- Network management

TECHNOLOGY TRENDS

PeopleSoft is considered the vendor of choice for the Enterprise Resource Planning (ERP) system. PeopleSoft's PeopleTools are considered to be a strategic development platform. A system assessment will be conducted in FY03 to determine the current needs of the Laboratory for automation in the budgeting area, and to identify possible solutions for supplementing, augmenting, or possibly replacing our current systems. This will include a reexamination of Janus, PeopleSoft, and IRIS as tools for future budget work.

Future trends include the continued upgrade of all business software to Web-based, thin-client technology. Vendor-supplied software, such as HRIS Release 8 or MRO Maximo Release 5, will be Web enabled. LETS Lite, which is Java-based and developed in-house, will be piloted in FY03. PMTS, which is supported by Oak Ridge, will be replaced with in-house-developed software using Java and JSP.

Vendors of Web-deployed applications are abandoning the heavy Java client in favor of back-end (server-side) Java processing to deliver a lightweight, non-Java (HTML, JavaScript, JScript) GUI to the client. It appears that Oracle is not planning to move in this direction.

Electronic commerce is also an emerging trend that will impact the way Berkeley Lab buys products and services. The Laboratory's business systems must facilitate the ordering and payment processes using appropriate technologies. PeopleSoft eProcurement addresses this need and positions the Laboratory for continuing competitiveness in this area.

Data mining, online analytical processing (OLAP), data analysis, and visualization of corporate data are areas in which opportunities might exist. These are all elements of the future enterprise decision support system. The data warehousing delivery mechanism needs business intelligence, ad hoc query and reporting, and decision support analysis tools. Microstrategy, Cognos, and Brio are examples of products that could be considered for this purpose.

Another technology trend that presents opportunities for the Laboratory is the use of enterprise business portal and content management applications. PeopleSoft is the vendor of choice for Berkeley Lab. The PeopleSoft portal will bring the Laboratory forward in this arena. Plumtree, Interwoven, Vignette, and Pipeline are among the industry leaders in content management and enterprise portal software. Digital Signatures is another area for exploitation.

RECOMMENDATIONS

- Develop all new in-house applications with Web-based, thin-client technology.
- Upgrade all vendor-supplied software to Web-based, thin-client technology.
- Where economically feasible, evolve all in-house developed client/server systems to Web-based, thin-client technology.
- Upgrade data warehousing maintenance and delivery technology.
- Implement portal technology, including PeopleSoft Portal.
- Use the Microsoft ASP/COM technology for rapid application deployment projects until similar capabilities using JSP can be evaluated.
- Review the .NET initiative as the benefits become clearer.
- Avoid thick-client applications based on a JVM. Develop using thin-client techniques with middle-tier business logic and software that uses HTML and XML for client-side work.
- Evaluate the potential for a Java-based development environment using JSP, and an IDE such as the one provided by Oracle’s JDeveloper or Borland’s JBuilder.
- Utilize PeopleTools for software that is tightly integrated into the PeopleSoft financial and human resource suites of programs.
- Define and publish a software design and development guideline (or update the one that now exists).
- Build or acquire applications that support a thin-client Web deployment model.
- Phase out the use and support of FileMaker Pro for corporate data applications. Evaluate alternatives to FileMaker Pro if a substitute can be identified that provides easily, centrally managed data.
- Continue to use NAL in support of legacy client/server applications until a Web-based method can be researched, or until these systems are migrated to Web applications.

Support Services

DESIRED STATE

- Effective and reliable support of remote users of Berkeley Lab systems.
- An integrated, cost-effective, high-quality support system (comprised of the Help Desk and all Tier II support groups) that consistently provides superior support for desktop computer systems, corporate business applications, and infrastructure services, such as e-mail and calendar, to all of the Laboratory's employees, no matter what group within ITSD actually performs the service.

CURRENT STATE

- A central Help Desk and Mac/PC desktop support group are available to support the Laboratory's standard hardware and software needs.
- A mature workflow system (Remedy) is in place, but it has limited Web access for use by the central support group. Conversion from Remedy 4 to 5.x will provide a Web component using JSP technology.
- A first-generation Web-based support area (with FAQs) is in place, but needs to be modernized.
- Oracle database support is available to the Laboratory through ISS.
- Desktop and server management (UNIX, Novell, NT) is available.
- Backup services are available.
- Centrally managed backups for UNIX systems are available but underutilized. Recently, a conversion from Legato to VERITAS, the acquisition of additional capacity, and the lowering of prices have begun to expand the customer base. MacDumps is being phased out as Macintosh users convert to the VERITAS system.
- On-site support for Laboratory customers during work hours is the norm. Very limited support is currently provided for remote users at home or on travel.
- Licenses for commonly used software are acquired through site licenses and volume discounts. For example, Norton is covered by a site license, and LabView is an example of a software product for which we receive volume discounts. A large number of Exceed licenses were purchased under a bulk purchasing agreement and distributed on a recharge basis. Current site licenses include:
  - Norton Antivirus
  - WinZip
  - Netscape Client and Server
  - Novell Client and NOS
  - Steltor Client and Server

  - Solaris
  - Legato NetWorker (backups)
  - SSH (from F-Secure Corp., formerly Data Fellows)
  - Mac OS
  - Ghost (Symantec)
  - Trend-Interscan (VirusWall)
  - Exceed
  - VMware (Acquired by the UNIX group)
  - LabVIEW
  - Timbuktu (only 100 licenses now being maintained)
  - Lotus Notes
  - Microsoft Office (via the standard load)
  - Windows Operating Systems
- One hundred licenses for Timbuktu remote control software were bought several years ago and remain under a maintenance agreement.
- The Network Services Group provides remote access to Laboratory computers and maintains approximately 1,000 user accounts. PPP, ISDN, and DSL are all supported.
- The Information Applications group in ISS provides custom Web development.
- ISS provides a Laboratory-wide application delivery service for OPS business systems.

TECHNOLOGY TRENDS

Procurement Vehicles

Procurement Card is the easiest and most cost-effective method of procurement today. However, it cannot be used to procure services that are accomplished on site (due to indemnification issues relating to possible injuries while on the job). In addition, it can only be used to buy standard PCs.

Hardware/Software Troubleshooting and Repair

The Mac/PC Support Group provides on-site service for desktop systems. Increasingly, the support is being offered as a matrix arrangement in which a resource is dedicated to an organization. Two-thirds of the staff operates this way. There is a significant downward trend in the use of time- and materials-based support.

The UNIX Support Group offers a similar service for UNIX platforms. For the past several years, most of the work has been on a service-level agreement basis. Time and materials is a much smaller percentage of the total workload.

Central Help Desk

The Central Help Desk supports CIS, ISS, and standard desktop applications. Unless staff is increased or a self-help knowledge base is deployed, service levels will not improve. (The volume of calls at peak times currently approaches the maximum that can be handled.)

Most of the types of requests for help appear to be Berkeley Lab–specific, and not generic questions that any help desk professional outside the Laboratory would be able to answer (such as questions on Microsoft Office).

Training and organization of methods and procedures are still first-generation. Better use of the Web and modern audio/visual content will assist training of staff and provide self-help for users.

The Help Desk should be included in the planning for Laboratory-wide system software implementations. For example, the new Procurement Receiving Payables (PRP) application team worked with the Help Desk staff prior to rollout.

The Laboratory's dependency on the Help Desk is increasing and the effectiveness of the staff is growing, with a significant increase in the use of tools to allow remote control of a customer's machine.

End-to-End Service Model

End-to-end service for remote users is a key issue. The way we provide workstation and software support to remote users at home, on campus, and on travel needs to be upgraded to address the increased volume and variety of remote access.

Laptop, PDA, and cell phone device use is increasing due to improvements in functionality and more aggressive pricing. This trend supports the increased need for remote access to the Laboratory from home or while on travel.

Standardization in offsite workstations would help make service more reliable. Documentation instructing the users on what is available, how to resolve problems, and whom to ask for help would facilitate improvement.

Training

On-site training for popular desktop software is provided by CompUSA. Recently, courses in Web and desktop publishing software were added to the course selections. We need to do more frequent reviews of popular software and develop training plans accordingly.

The University of California Office of the President is reviewing the acquisition and delivery of training for all three national laboratories. Insourcing may be an option from centers of excellence. In addition, new vendors for outsourcing popular classes may be recommended.

New employee training does not address computing services. This is typically provided by current employees as part of "on-the-job" training. This may not be the most cost-effective solution. A new employee computing-services class may be beneficial, particularly for the administrative staff.

Time-and-Material Support Model

The time-and-material support model is decreasing in favor of service-level agreements for specific machines, or matrixed agreements where a CIS staff member is “bought” part- or full-time by a customer organization.

Software Acquisition

Microsoft is dominating the PC software business and does not offer significant discounts to its product line. Site licenses are expensive. GSA contracts are available for procurement.

RECOMMENDATIONS

- Do a formal review of class offerings based on the products recommended by this document.
- Develop a new employee computer orientation class highlighting computing services and commonly used products such as e-mail and calendar.
- Continue to expand the customer base for Central Backups.
- Improve support to offsite customers who access Laboratory computing facilities remotely.
- Standardize remote workstations.
- Develop better Webcentric methods for helping users.
- Make ITSD Web site pages consistent and easy to find.
- Develop incentives for staff to use the standard desktop and laptop machines.

Multimedia, Publishing, and Archiving Services

DESIRED STATE

- Web access to the Technical and Electronic Information Department's (TEID) multimedia assets, including video and graphics.
- Real-time customer access to project management reports of TEID work, including workflow and recharges.
- Continued support for best industry standards (software and hardware) in the creative production business. Range of tools includes Mac platform, high-end large-format printing, digital video creation, DVD production, etc.
- Tight integration in use of enterprise-wide collaborative workgroup system, document management system, and records management system.
- Web access to all library services, including journals, interlibrary loan, 24/7 reference service.
- Web access to reports database as well as full text reports.
- Archives and Records Office database is robust and DOE-compliant, with Web browser interface.
- Easy migration of data between Reports Database and EndNotes users.

CURRENT STATE

- Migrating current image archive database to Oracle (with browser access).
- Migrating Archives and Records database to latest version of Microsoft Access.
- Using BASISplus for Report Coordination database and TECHLIBplus for Library automation system (both with browser access).
- TEID's current business management software, Job Order, does not provide real-time customer access to project management reports.
- Utilizing Macintosh desktop workstations and production software such as Final Cut Pro that only runs on a Macintosh.
- Providing search and playback access to TEID streaming "Real" videos and related metadata via the Virage system.
- Creating and delivering QuickTime content.
- Making hardware upgrades to Novell (TEIDNOV1) and UNIX servers (TEID Web server).
- Using high-end photo-quality large-format printer, EPSON 9500, and its associated raster input processor (RIP) to produce poster-size output.
- Purchase of 24/7 Reference, a virtual, Web-based reference service, for an initial limited implementation (it will not be staffed 24/7). 24/7 Reference is a customized set of software

tools that lets library patrons ask questions and get answers in real time, on the Internet, from live reference staff.

TECHNOLOGY TRENDS

- Some libraries are joining in collaborative agreements and pooling staff to offer their 24/7 reference services around the clock.
- EndNotes is a bibliography management tool valuable to scientists for managing citations, curriculum vitae, etc. EndNotes is becoming the de facto standard at the Laboratory.
- PDF is an increasingly popular file format and industry standard for production, and is the desired file format for DOE.
- OpenType is becoming the font industry standard. OpenType is the result of a joint effort between Adobe and Microsoft to address cross-platform compatibility issues and to begin eliminating font problems. See http://www.adobe.com/type/opentype/main.html.
- More journals and other source materials are becoming available electronically. The cost of access to electronic resources is continuing to increase.
- Technology developers are responding to increased demand for desktop access to multimedia assets, from text to images to animation to video.
- Demand is increasing at the Laboratory for QuickTime production services, including QTVR with maps and sound overlays.

RECOMMENDATIONS

- Establish a QuickTime server.
- Determine if volume or site license for full version of Adobe Acrobat is warranted.
- Determine if volume or site license for EndNotes is warranted.
- Establish training courses in Adobe Acrobat.
- Investigate the potential for OpenType fonts as a standard at the Laboratory.
- Add QuickTime and Real One Player on the standard load.
- Investigate the possibility of acquiring a Z39.50-compliant server to allow easy migration of data between Reports Database and EndNotes users.
- Migrate Archives and Records Office database from Microsoft Access to DOE-compliant records management system or, if that is too expensive, to Oracle.
- Evaluate alternatives to JobOrder.

.

Appendix A:
LBLnet Technologies and Systems

INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERING (IEEE) STANDARDS 802.3

10BaseT	10Mbps
10BaseTX	10Mbps
100BaseT	100Mbps
100Base-FX	100Mbps
1000Base-TX	1Gbps
1000Base-SX	1Gbps
1000Base-LX	1Gbps
802.3ae	10Gbps

LIST OF INTERNET REQUEST FOR COMMENTS (RFCs)

The RFC document series is a set of technical and organizational notes about the Internet, dating back to 1969. Memos in the RFC series discuss many aspects of computer networking, including protocols, procedures, programs, and concepts.

The following RFCs are the basis of LBLnet's specifications and protocols:

Network Services

1591 Domain Name System Structure and Delegation. J. Postel. March 1994.

2136 Dynamic Updates in the Domain Name System (DNS UPDATE). P. Vixie, Ed., S. Thomson, Y. Rekhter, J. Bound. April 1997.

2137 Secure Domain Name System Dynamic Update. D. Eastlake. April 1997.

2117 Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification. D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei. June 1997.

Routing Protocols

1126 Goals and functional requirements for inter-autonomous system routing. M. Little. Oct-01-1989.

1771 A Border Gateway Protocol 4 (BGP-4). Y. Rekhter, T. Li. March 1995.

1583 OSPF Version 2. J. Moy. March 1994.

Remote Access

2138 Remote Authentication Dial In User Service (RADIUS). C. Rigney, A. Rubens, W. Simpson, S. Willens. April 1997.

2139 RADIUS Accounting. C. Rigney. April 1997.

LAN and Remote Access

2131 Dynamic Host Configuration Protocol. R. Droms. March 1997.

2132 DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997.

Next Generation LAN (IPv6)

2460 Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998.

2461 Neighbor Discovery for IP Version 6 (IPv6). T. Narten, E. Nordmark, W. Simpson. December 1998.

2462 IPv6 Stateless Address Autoconfiguration. S. Thomson, T. Narten. December 1998.

2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. A. Conta, S. Deering. December 1998.

2464 Transmission of IPv6 Packets over Ethernet Networks. M. Crawford. December 1998.

1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses. S. Cobb. December 1995.

Network Management

2013 SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2. K. McCloghrie, Ed. November 1996.

Appendix B:
Technical Architecture Working Group

Stephen Abraham
Dennis Baker
Greg Balin
Tammy Campbell
David Edgar
Richard Gregory
Daisy Guerrero
Gary Jung
Rob Macfarlane
Vickie Ng
Richard Nosek
Jose Olivares
John Pon
Erik Richman
Mark Rosenberg
Gene Schultz
Ted Sopher
Linda Suarez
Charles Verboom
Jeff Willer

Advisory Committee:
Ali Belkacem
Alessandra Ciocio

Technical Editors:
Theresa Duque
John Hules
Julie McCullough

Word Processor:
Jean Wolslegel